DRAFT

GUIDE TO OSCAL-BASED FEDRAMP SYSTEM SECURITY PLANS

Version 1.0

November 27, 2019

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
11/27/2019	Initial Publication	1.0	FedRAMP PMO
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to Contact Us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@FedRAMP.gov.*

For more information about FedRAMP, see https://FedRAMP.gov.

TABLE OF CONTENTS

1. OVERVIEW

FedRAMP System Security Plans (SSPs) expressed using the NIST Open Security Controls Assessment Language (OSCAL) must follow the FedRAMP standard for the core OSCAL syntax.

This document provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SSP files. Our goal is to enable your organization to develop tools that will seamlessly ensure these standards are met so your security practitioners can focus on SSP content and accuracy rather than formatting and presentation.

1.1. Who Should Use This Document?

This document is intended for technical staff and tool developers implementing solutions for importing, exporting, and manipulating OSCAL-based FedRAMP SSP content.

1.2. Basic Vocabulary

XML and JSON use different terminology. NIST defines OSCAL using a special file that generates all the XML and JSON resources. Within this file, NIST uses a third set of terminology intended to be agnostic to any particular format.

We use the following terms to keep the document concise, rather than constantly clarifying the XML and JSON terms:

TERM	XML EQUIVALENT	JSON EQUIVALENT
`Field`	A single element or node that can hold a value or an attribute	A single object that can hold a value or property
`Flag`	Attribute	property
`Assembly`	A collection of elements or nodes. Typically, a parent node with one or more child nodes.	A collection of objects. Typically, a parent object with one or more child objects.

1.3. Data Formats

The examples provided here are in XML; however, FedRAMP accepts XML or JSON formatted OSCAL-based SSPs. NIST offers a utility that provides lossless conversion of OSCAL-compliant files between XML and JSON in either direction.

This means your organization can submit to FedRAMP using either format, and FedRAMP can accept it.

To convert SSP files, you must have:

- An XSLT 3.0 and XPath 3.1 processor
- The NIST-provided XSLT file for converting a JSON SSP to XML
- The NIST provided XSLT file for converting an XML SSP to JSON

1.4. OSCAL-based FedRAMP Template

FedRAMP offers an OSCAL-based SSP shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that shell file. The OSCAL-based FedRAMP SSP Template is available here:

[NEED URL TO TEMPLATE - ONCE LOCATION HAS BEEN ESTABLISHED]

1.5. XPath References

Except where noted, all XPath references in this document are based on XPath 2.0.

XPath 1.0 is available in the DOMdocument model of most modern programming languages, and XPath 2.0 can be added with third-party libraries; however, most XPath queries in this document can be translated from XPath 2.0 to XPath 1.0 by simply pre-pending a namespace specifier to each of the elements in the XPath query.

Sample PHP Code to Prepend Namespace (XPath 2.0 to 1.0 Conversion)

```
function AddNamespace2xpath($query, $ns) {
	$temp = "";
	$q_len = strlen($query);
	$prev_char = "";

	for($i=0; $i < $q_len ; $i++) {
		$cur_char = substr($query, $i, 1);
		if ($prev_char === '/') {
			if (ctype_alpha($cur_char)) {
				$temp .= $ns . ":";
			};
		}
		$temp .= $cur_char;
		$prev_char = $cur_char;
	}

	return $temp;
}
```

2. WORKING WITH OSCAL FILES

This section covers several important concepts and details that apply to OSCAL-based FedRAMP SSP files.

2.1. Sequence and Hierarchy Are Important

At any given level, the syntax validation rules for XML-based OSCAL files requires the fields and assemblies to appear in a particular order. Further, the hierarchy of field placement within assemblies is important. The same field name will be interpreted differently in different assemblies. For example, the `title` field under metadata is the document title, while the `title` field under role gives a human-friendly name to that role.

OSCAL files will fail the basic NIST validation if this is not honored. Fortunately, NIST's documentation presents the fields and assemblies in the correct sequence.

Always use the sequence found here:

https://pages.nist.gov/OSCAL/documentation/schema/ssp/xml-model-map/

2.2. Multiple Layers of Validation

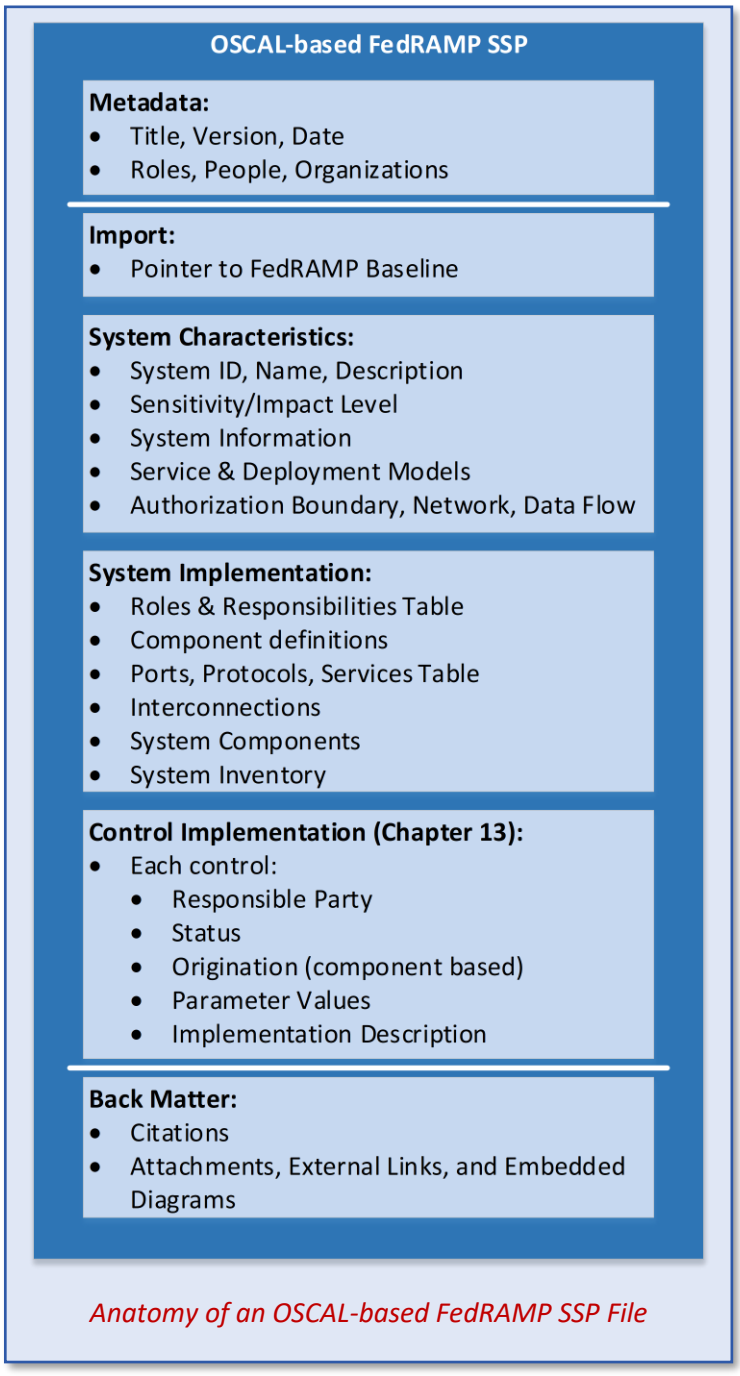
There are several layers at which an OSCAL file can be considered valid.
FedRAMP requires all layers be satisfied.

LAYER	DESCRIPTION
Well-Formed	The XML or JSON file follows the rules defined for that format. Any tool that processes the format will recognize it as "well-formed", which means the tool can proceed with processing the XML or JSON. XML: https://www.w3.org/TR/REC-xml/ JSON: https://json.org/
OSCAL Syntax	The XML or JSON file uses only tagging that is defined by NIST for OSCAL. NIST publishes schema validation tools to verify syntax compliance: XML Schema Definition Language (XSD) 1.1: OSCAL SSP XML Validation File JSON Schema, draft 07: OSCAL SSP JSON Validation File
OSCAL Content	Currently NIST only enforces declarations, using the validation files above. This means defining a limited set of acceptable values for certain fields. For example, NIST declared the following as the only acceptable values for the impact levels for information types: "fips-199-low", "fips-199-moderate", and "fips-199-high". Any other value will raise an error when validating the file using the NIST schema tools above. In the future, NIST intends to publish content enforcement mechanisms, such as Schematron mechanisms. This will enforce rules such as, "If this field is marked 'true', a value must be provided for the next field."
FedRAMP Syntax Extensions	NIST built a language they believe represents the commonality of most cybersecurity frameworks and provided the ability to extend the language for framework-specific needs. FedRAMP makes use of these extensions. NIST provides `prop` and `annotation` fields throughout its most assemblies, always with a `name`, `class`, and `ns` (namespace) flag: `<prop name="" class="" ns="">Data</prop>` In the core OSCAL syntax, the `ns` flag is never used. Where FedRAMP uses these to extend OSCAL, the value for `ns` is always 'fedramp' (case sensitive). When `ns='fedramp'` the `name` (and optionally `class`) flags are as defined and used by FedRAMP.
FedRAMP Content	Today, FedRAMP content is enforced programmatically. FedRAMP will evaluate the use of Schematron (above) for future FedRAMP validation efforts.

2.3. OSCAL's Minimum File Requirements

Every OSCAL-based FedRAMP SSP file must have a minimum set of required fields/assemblies, and must follow the OSCAL SSP core syntax found here:

https://pages.nist.gov/OSCAL/documentation/schema/ssp/



Anatomy of an OSCAL-based FedRAMP SSP File

In addition to the core OSCAL syntax, the following FedRAMP-specific implementation applies:

- A FedRAMP SSP must include all the sections shown in the diagram to the left.
- At a minimum, the FedRAMP SSP must have at least one defined component, which represents the system as a whole. This is addressed in more detail in the system inventory.
- A leveraged authorization is defined as a component, if the system is leveraging another FedRAMP-authorized system.

The table below shows an empty OSCAL SSP, based purely on the NIST syntax; however, FedRAMP requires much more in a minimum file. The latest OSCAL-based FedRAMP SSP template file can be found here:

> [We need to decide where to host the OSCAL-based FedRAMP SSP template and provide a link to it here.].

An Empty OSCAL SSP Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<system-security-plan xmlns="http://csrc.nist.gov/ns/oscal/1.0"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   id="[generated-uuid-here]">
   <metadata>
      <title>System Security Plan (SSP)</title>
      <last-modified>2019-11-27T00:00:00.00-05:00</last-modified>
      <version>0.0</version>
      <oscal-version>1.0-Milestone2</oscal-version>
   </metadata>
   <import-profile href="baseline-profile.xml" />
      <system-characteristics>
         <system-id>Unique System Identifier</system-id>
         <system-name>System's Name</system-name>
         <description><p>Description of system's Name</p></description>
         <security-sensitivity-level>moderate</security-sensitivity-level>
         <system-information>
            <information-type id="info-type-01" name="Name">
               <description><p>Description</p></description>
               <confidentiality-impact>
                  <base>fips-199-moderate</base>
               </confidentiality-impact>
               <integrity-impact>
                  <base>fips-199-moderate</base>
               </integrity-impact>
               <availability-impact>
                  <base>fips-199-moderate</base>
               </availability-impact>
            </information-type>
         </system-information>
         <security-impact-level />
         <status state="operational" />
         <authorization-boundary>
            <description><p>Description</p>
         </description>
      </authorization-boundary>
      </system-characteristics>
      <back-matter />
</system-security-plan>
```

NOTES:

- The first line ensures UTF-8 is used for character encoding. Other encoding options will create unpredictable validation results.

Below are a few important queries, which enable a tool to obtain critical information about an OSCAL file.

XPath Queries

OSCAL syntax version used in this file:
`/*/metadata/oscal-version`

Last Modified Date/Time:
`/*/metadata/last-modified`

Unique Document ID:
`/*/system-security-plan/@id`

Document Title:
`/*/metadata/title`

NOTES:

- For full OSCAL compliance, any time the document changes:
  - the `id` flag should be updated with a unique identifier; and
  - the `last-modified` field should be updated with the current date and time.
- Tools that work with updates to an OSCAL file should rely on the UUID value provided by the `id` flag, and `last modified` field as an easy method of knowing the file has changed.
- NIST intends to add a cryptographic hash feature in the future; however, this is not available today.
  - While tool developers are encouraged to perform as much integrity checking as possible, it is important to note the content of a JSON or XML file may not have changed, yet a different cryptographic hash could be produced as a result of things like code formatting, which might have different indentation, or change the sequence of flags.
- Tools reading an OSCAL file should verify the `oscal-version` field to determine which published syntax is used.
  - NIST intends to enable backward compatibility as much as possible; however, this is not guaranteed, especially before a full final 1.0 version of OSCAL.
  - NIST intends to keep all formally published schema validation files available, which enables an organization to validate files based on older versions of OSCAL.

2.4. Assigning Identifiers

There are two types of identifiers in OSCAL:

- ID: identifies a field or assembly, and must be unique within an OSCAL file
- ID References (ID Ref): points to a field or assembly using its identifier.

IDs appear as an "**id**" XML attribute or JSON property to a data field or assembly. Examples include:

- `<interconnection id="ic-001">`: Uniquely identifies the interconnection
- `<party id "party-csp">`: Uniquely identifies the party

ID references usually appear with a name and hyphen in front of the "id", and are typically an attribute/ property, but are sometimes a field. The name of an ID reference field typically reflects the name of the field or identifier.

Examples include:

- `<responsible-party role-id="role-ssp-by">`: points to the role identified by the ID, "role-ssp-by".
- `<implemented-requirement id="imp-req-01" control-id="ac-2">`: points to the control identified by "ac-2".

Throughout the OSCAL syntax, if an ID attribute/property is present, it is typically required.

IDs must be unique within the entire OSCAL file, including any IDs associated with imported information. For example, "ac-1" is the ID for the AC-1 control in the imported FedRAMP baseline, which means "ac-1" cannot be used as an ID for anything else within the OSCAL file.

2.5. Special Characters in OSCAL

Characters, such as ampersand (&), greater than (>), less than (<), and quotes require special treatment in OSCAL files, depending on the format. For a complete list of special characters and the appropriate treatment for each format, please visit:

https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#specialized-character-mapping

2.6. Handling of OSCAL Data Types

OSCAL fields and flags have data types assigned to them. NIST provides important information about these data types here:
https://pages.nist.gov/OSCAL/documentation/schema/datatypes/

The following sections describe special handling considerations for data types that directly impact FedRAMP SSP content in OSCAL.

2.6.1. Date and Time in OSCAL Files

Except where noted, all dates and times in the OSCAL-based SSP must be in an OSCAL dateTime-with-timezone format as documented here:

https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#datetime-with-timezone

This means all dates and times must be represented in the OSCAL file using following format, unless otherwise noted:

`"Y-m-d\TH:i:s.uP"` (See HERE for formatting codes.)

For example, a publication date of 5:30 pm EST, January 10, 2020 must appear as 2020-01-10T17:30:00.00-05:00

This includes:

- Numeric Year: Four-digits
- A dash
- Numeric Month: Two-digit, zero-padded
- A dash
- Numeric Day: Two digit, zero padded
- The capital letter “T” (Do not use lower case)
- Hour: Two digit, zero-padded, 24-hour clock (Use 18 for 6:00 pm)
- A colon
- Minute: Two digit, zero-padded
- A colon
- Seconds: Two digit, zero-padded
- A decimal point
- Fractions of a second: two or three digits, zero padded

Followed by either:

- A capital letter Z to indicate the time is expressed in Coordinated Universal Time (UTC)

OR:

- A plus or minus representing the offset from UTC
- Hour Offset: Difference from UTC, two-digit, padded
- A colon
- Minutes Offset: Difference from UTC, two-digit, padded

This is only for *storing* dates in the OSCAL file. NIST syntax verification tools will generate an error if this format is not found.

Tool developers are encouraged to *present* dates as they have historically appeared in the FedRAMP SSP template. In other words, tools should convert "`2020-03-04T00:00:00.00-05:00`" to "`March 4, 2020`" when presenting the publication date to the user.

Please use the appropriate UTC offset in your region. If you are storing a date and padding the time with zeros, you may also pad the UTC offset with zeros.

2.6.2. Working With href Flags

Several OSCAL fields contain `href` flags. All OSCAL-based `href` flags are uniform resource identifiers (URIs) formatted according to section 4.1 of RFC3986. When assembling or processing an OSCAL-based FedRAMP SSP please consider the following:

Absolute Paths: When using an absolute path within a FedRAMP SSP, the path must be publicly accessible from any location on the Internet, to ensure agency and FedRAMP reviewers can reach the information.

Tool developers are encouraged to validate paths before storing them in OSCAL files and raise issues to users if paths are not reachable.

Relative Paths: All relative paths are assumed to be based on the location of the OSCAL file, unless tools are explicit as to other handling. Sensitive external documents should travel with the SSP and be linked using a relative path.

Internal Locations: These URI fragments appear as just a hashtag (#) followed by a name, such as "#att-diagram-1". The notation points to a location internal to the document itself and is most commonly used in an OSCAL-based FedRAMP SSP as a pointer to `resource` assemblies.

If only a fragment is present, the OSCAL tools must strip the hashtag (#) and treat the remaining string as an ID internal to the OSCAL file itself. For example, the following OSCAL content contains an `href` flag with a URI fragment:

URI Fragment Example

```
<system-characteristics>
   <authorization-boundary>
      <diagram id="dia-authorization-boundary-1">
         <link href="#att-diagram-boundary-1"/>
         <caption>Authorization Boundary Diagram</caption>
      </diagram>
   </authorization-boundary>
</system-characteristics>
```

When a tool processes the above example, it should look inside the document for a field or assembly with an ID of "`att-diagram-boundary-1`". This can be accomplished with the following XPath query:
`//*[@id="att-diagram-boundary-1"]`

If this is found to point to a resource assembly, see the *Attachments and Embedded Content in OSCAL Files* section for additional handling.

The name of the field or assembly referenced by the above URI fragment can be determined using the following XPath query:

```
//*[@id="att-diagram-boundary-1"]/name()
```

The above query will return "`resource`", if the ID points to a `resource` assembly.

2.6.3. Markup-line and Markup-multiline Fields in OSCAL

As with most machine-readable formats, most of OSCAL's fields are intended to capture short, discrete pieces of information; however, sometimes users require content to be formatted using features such bold, underline, and italics.

NIST provides two types of fields for this purpose:

- **markup-line**: Allows for formatting within a single line of text.
- **Markup-multiline**: Allows all the markup-line formatting, plus allows multiple lines, ordered/ unordered lists, and tables.

HTML is used to format XML-based OSCAL files, while Markdown is used to format JSON-based OSCAL files.

NIST has implemented only a subset of formatting tags from these standards. For a complete list of markup-line and markup-multiline features, please visit:
https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-data-types

Both *markup-line* and *markup-multiline* allow:

- emphasis and important text
- inline code and quoted text
- sub/super-script
- images and links

Markup-multiline also supports:

- Paragraphs
- Headings (Levels 1-6)
- Preformatted text
- Ordered and Unordered Lists
- Tables

2.6.4. Working with Markup-multiline Content

No special handling is required to work with markup-multiline content in JSON; however, XML-based markup-multiline fields require all content to be enclosed in `<p>`, `<h1>` - `<h6>`, `<ol>`, `<ul>`, `<pre>`, or `<table>` tags. You may have several of these within the field.

The following examples offer correct and incorrect representations of Markup-multiline content.

The example below is a common miss-use of markup-multiline. The description contains text, but the text is not enclosed in one of the required tags. This will produce an error when checked with the OSCAL schema.

Incorrect Markup-multiline Representation

```
<system-characteristics
   <!-- cut -->
   <description>The xyz system performs ...</description>
</system-characteristics>
```

The simplest way to correct the error is to enclose the text in tags, within the `description` field.

Correct Markup-multiline Representation

```
<system-characteristics
   <!-- cut -->
   <description><p>The xyz system performs ... </p></description>
</system-characteristics>
```

The example below demonstrates a correct use of markup-multiline in XML. Please note, the inclusion of a `<p />` tag on a line by itself inserts an empty paragraph. Within XML and HTML, this is treated as a shortcut, and is interpreted as "`<p></p>`"

Correct Markup-multiline Representation

```
<system-characteristics
   <!-- cut -->
   <description>
      <p>The <b>xyz system</b> performs ... </p>
      <p>The xyz system further supports ... as follows:</p>
      <table>
         <tr>
            <td>Cell A1</td>
            <td>Cell B1</td>
         </tr>
         <tr>
            <td>Cell A2</td>
            <td>Cell B2</td>
         </tr>
      </table>
      <p />
      <h1>Big Header</h1>
      <p>More detail</p>
      <p><img alt="alt text" src="url" title="title text"/></p>
   </description>
</system-characteristics>
```

Please also note, all content is enclosed in one of the supported high-level tags (`<p>`, `<h1>` - `<h6>`, `<ol>`, `<ul>`, `<pre>`, or `<table>`).

For more information, please visit:
https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-data-types

2.7. Citations, Attachments and Embedded Content in OSCAL Files

All citations, attachments, and embedded content are handled in the back-matter section of the OSCAL file as a `citation` or `resource` assembly. This includes logos, diagrams, policies, procedures, plans, and interconnection security agreements (ICAs). Each `citation` or `resource` may be referenced from anywhere in the OSCAL file, using its citation ID or resource ID. FedRAMP prefers Base64-encoding for diagrams, such as those related to the authorization boundary, network architecture, and data flows.

```
<back-matter>
   <!-- citation -->
   <resource id="csp-logo">
      <desc>CSP Logo</desc>
      <rlink href="./logo.png" media-type="image/png" />
      <rlink href="./logo.jpg" media-type="image/jpeg" />
      <base64>--- base64 content cut ---</base64>
   </resource>
</back-matter>
```

Resources may be expressed as:

- a link to external file (`rlink`);
- `base64`-encoded data within the OSCAL file;
- both; or
- neither.

OSCAL allows multiple rlink fields for the same resource, which are intended to provide options such as links to the same content in different formats, or low- and high-resolution versions of the same graphic.

> At the time of writing, the NIST OSCAL syntax validation tools do not allow both `rlink` and `base64` fields to be present that the same time. NIST is investigating this and is expected to resolve the issue. This section will be updated when the issue is closed by NIST as tracked HERE.

There is no OSCAL rule which governs how a tool should handle a situation where both the rlink and base64 fields and/or where multiple rlink fields are present for a single resource.

FedRAMP tools will always give preference to base64-encoded content. If the `base64` field is present with valid content, FedRAMP tools will ignore all `rlink` fields.

If the `base64` field is missing or invalid, FedRAMP tools will try the first `rlink` field. If that works, all remaining `rlinks` will be ignored. If the first one does not work, FedRAMP tools will try the second link, then the third. It will keep going until either a valid rlink is found, or no rlink fields remain.

CSPs should take care when using `rlink` fields to ensure all paths are relative to the OSCAL file's location itself, and the referenced items delivered to FedRAMP with the OSCAL file.

The `resource` assembly could be used with neither `rlink` nor `base64` embedded content. If citing a document that may be attached or embedded later, this approach may be used as a placeholder. If citing a document that will never be attached or embedded, use the `citation` assembly instead.

Using either the `citation` or `resource` assembly with the FedRAMP's additional properties (title, publication, and version), enables a CSP to reference a document by title, version, and date in one place, then reference it where needed throughout the OSCAL file. This way, the title, version and date can be updated in one place and will appear updated everywhere it is referenced.

3. FEDRAMP EXTENSIONS, DEFINED IDENTIFIERS, AND ACCEPTED VALUES

NIST designed the core OSCAL syntax to meet model cybersecurity information that is common to any organization and compliance framework. They recognized that each framework and organization may have unique needs. Instead of trying to provide a language that meets each of those unique needs, NIST gave organizations the ability to tailor OSCAL to address specific needs.

A summary of the FedRAMP extensions, defined identifiers, and accepted values appears in the FedRAMP OSCAL Registry.

FedRAMP has tailored OSCAL by specifying:

- **Extensions**: allow FedRAMP's OSCAL-based SSP to capture information that is not available in the core OSCAL SSP syntax.
- **Defined Identifiers**: FedRAMP defines several unique ID values that must be used in the ID flag of certain OSCAL fields and assemblies. This allows FedRAMP processing tools to find required information without human intervention.
- **Accepted Values**: For many fields, FedRAMP specifies a case-sensitive set of values. Only these values are recognized by FedRAMP processing tools.

3.1.1. FedRAMP Extensions

All FedRAMP extensions include a `ns` flag set to "`fedramp`". NIST only allows an organization to extend OSCAL-based SSP content using `prop` fields and `annotation` assemblies, and imposes the following fundamental requirements on OSCAL extensions:

- The organization establishes a unique name space identifier (`ns="fedramp"`), which is used to consistently tag all extensions from that organization.
- The organization is responsible for defining and managing all names (`name="direction"`) defined and tagged with the above name space identifier.

This allows each organization to create their own extensions in their own name space without concern for overlapping extension names.

NIST's core OSCAL `prop` fields and `annotation` assemblies have no `ns` flag. If an `ns` flag is present, it is an organization-defined extension.

For example, if the core OSCAL syntax has a status field, but both FedRAMP and the payment card industry (pci) require their own framework-specific status fields, each may define an extension with the `name="status"`, and assign their own `ns` flag. This results in three possible status fields as follows:

NIST OSCAL Status Representation
`<prop name="status">General Status</prop>`
XPath Query
`/*/prop[@name="status"][not(@ns)]`

When searching an OSCAL file for a `prop` or `annotation` extensions that is part of the core OSCAL syntax, developers must filter out any with an `ns` flag using the syntax above.

FedRAMP Status Representation
`<prop name="status" ns="fedramp">FedRAMP Status</prop>`
XPath Query
`/*/prop[@name="status"][@ns="fedramp"]`

(Possible) PCI Status Representation
`<prop name="status" ns="pci">CSA Status</prop>`
XPath Query
`/*/prop[@name="status"][@ns="pci"]`

* This is an example, and not intended to represent an actual PCI extension.

Tool developers must always refer to extensions using **both** the `name` and `ns` flags as a pair.

All FedRAMP extensions will appear as either:

```
<prop name="____" ns="fedramp">Value</prop>
```

or:

```
<annotation name="____" ns="fedramp" value="Value">
   <remarks><p>An optional remark about the value</p></remarks>
</annotation>
```

NOTE: The catalog and profile OSCAL models also allow the `part` assembly to be used for extensions. This is not currently the case for the SSP OSCAL model.

FedRAMP extensions are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

3.1.2. FedRAMP Defined Identifiers

To facilitate consistent processing, FedRAMP requires specific identifiers be used on several fields/ assemblies within the OSCAL file.

For example, every SSP must identify a system owner and an Information System Security Officer (ISSO). FedRAMP defines specific identifiers for these roles, and enables FedRAMP tools to easily identify the individuals associated with these roles.

FedRAMP defined identifiers are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

3.1.3. OSCAL and FedRAMP Accepted Values

To facilitate consistent processing, the value for some fields is limited to a list of *case-sensitive* acceptable values. For some fields, OSCAL defines acceptable values, which are enforced by OSCAL-based syntax validation mechanisms.

There are additional fields, where OSCAL syntax validation mechanisms will accept any value, but FedRAMP provides a limited list of *case-sensitive* acceptable values. Where defined, only these values are recognized by FedRAMP processing tools.

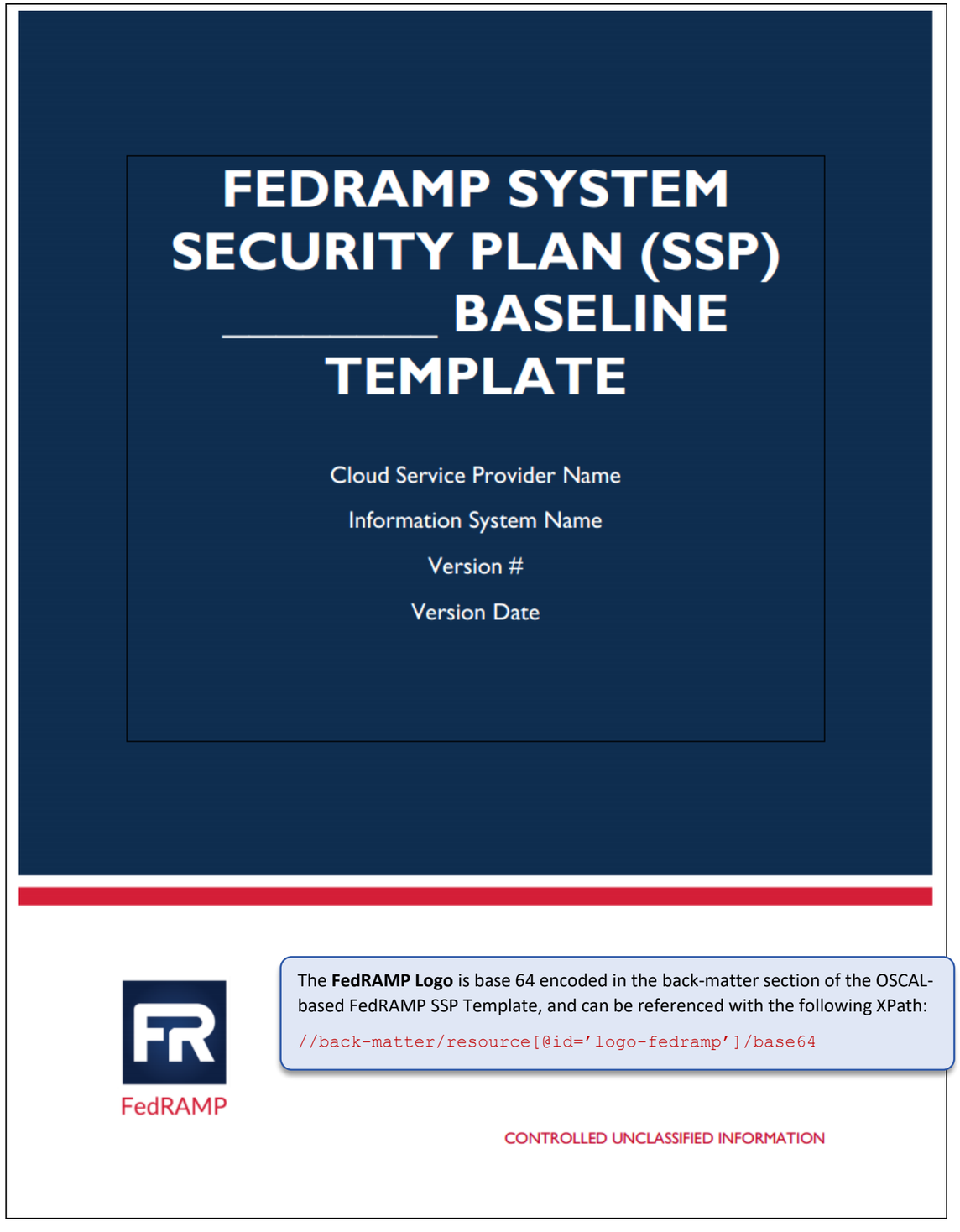
For example, every control requires an implementation status. FedRAMP only accepts one of five possible responses for this status, which must be provided using one of the specified choices.

FedRAMP accepted values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

4. SSP TEMPLATE TO OSCAL MAPPING

Each page of the SSP where content is provided by a CSP is represented in this section, along with OSCAL code snippets for representing the information in OSCAL syntax. There is also XPath syntax for querying the code in an OSCAL-based FedRAMP SSP represented in XML format.

The following pages are intended to be printed landscape on tabloid (11" x 17") paper.



4.1. SSP Title Page

Representation

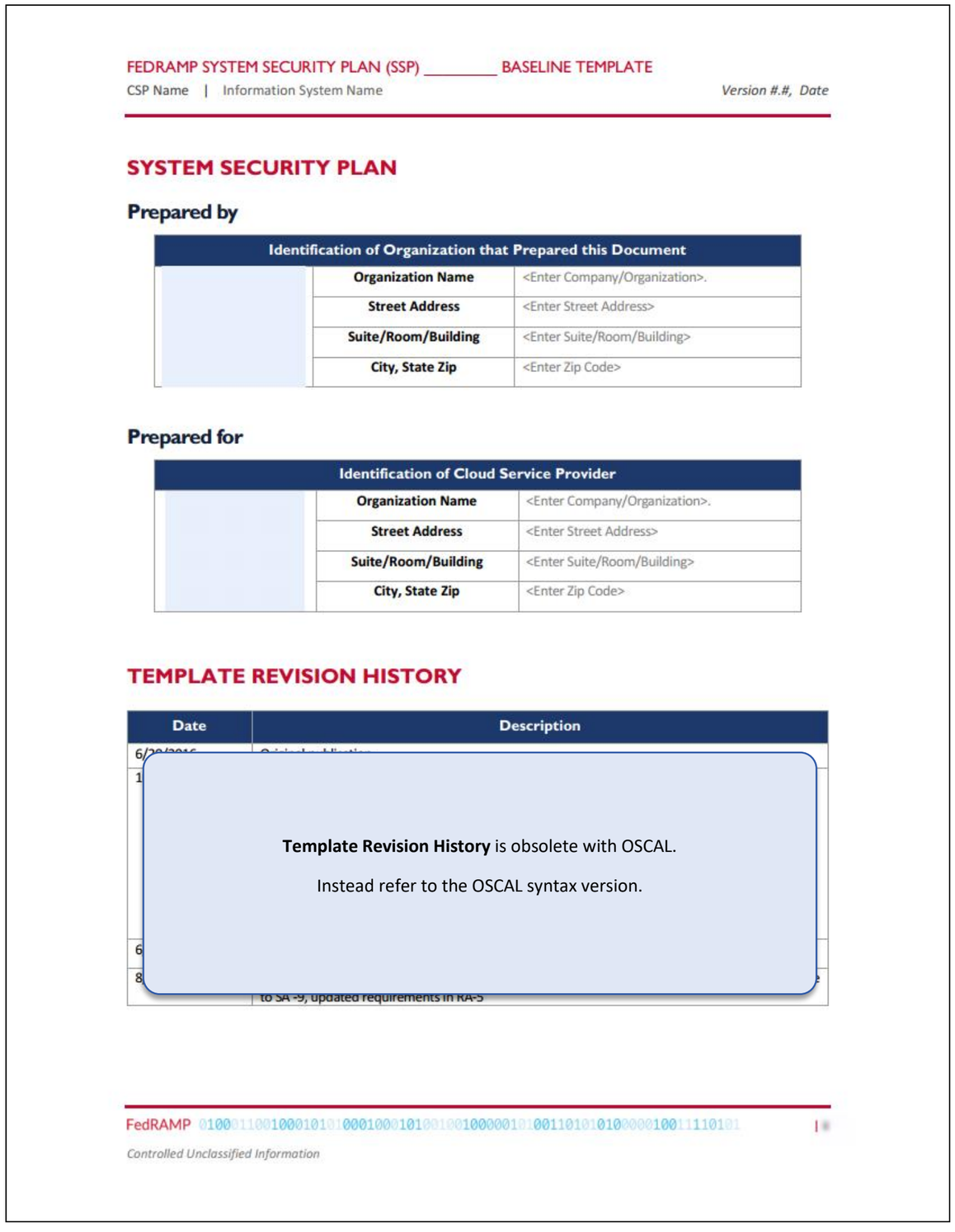
```
<metadata>
   <title>FedRAMP System Security Plan (SSP)</title>
   <published>2019-10-21T00:00:00.00-04:00</published>
   <last-modified>2019-11-27T00:00:00.00-04:00</last-modified>
   <version>0.0</version>
   <oscal-version>1.0-Milestone2</oscal-version>
   <prop name="marking" ns="fedramp">Controlled Unclassified Information</prop>
   <!-- role -->
   <party id="party-csp">
      <org>
         <org-name>Cloud Service Provider (CSP) Name</org-name>
         <short-name>CSP Acronym/Short Name</short-name>
      </org>
   </party>
   <!-- responsible-role -->
</metadata>

<!-- This must point to the appropriate FedRAMP Baseline -->
<import-profile href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml"/>

<system-characteristics
   <system-id identifier-type="https://fedramp.gov">F00000000</system-id>
   <system-name>System's Full Name</system-name>
   <system-name-short>System's Short Name or Acronym</system-name-short>
   <!-- description -->
</system-characteristics>
```

XPath Queries

```
CSP Name:
  /*/metadata/party[@id='party-csp']/org/org-name

Information System Name:
  /*/system-characteristics/system-name

SSP Document Published Version #:
  /*/metadata/version

SSP Document Published Date:
  /*/metadata/published

CSP's Logo:
  /*/back-matter/resource[@id='logo-csp']/base64

Document Sensitivity Label:
  /*/metadata/prop[@name="marking"][@ns="fedramp"]
```

NOTES:

- The import-profile field is required. There must always be a profile imported. All of the control definition statements, and parameter descriptions are imported via that profile.
- The correct URLs for each FedRAMP baseline appear in Appendix A. There are separate XML and JSON URLs for each baseline.



FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

SYSTEM SECURITY PLAN

Prepared by

Identification of Organization that Prepared this Document		
	Organization Name	<Enter Company/Organization>.
	Street Address	<Enter Street Address>
	Suite/Room/Building	<Enter Suite/Room/Building>
	City, State Zip	<Enter Zip Code>

Prepared for

Identification of Cloud Service Provider		
	Organization Name	<Enter Company/Organization>.
	Street Address	<Enter Street Address>
	Suite/Room/Building	<Enter Suite/Room/Building>
	City, State Zip	<Enter Zip Code>

TEMPLATE REVISION HISTORY

Date	Description
6/29/2016	Original publication
1	
6	
8	to SA -9, updated requirements in RA-5

Template Revision History is obsolete with OSCAL.

Instead refer to the OSCAL syntax version.

FedRAMP 0100011001000101010001000101001001000001010011010101000001001111010101 | 8

Controlled Unclassified Information

4.2. SSP Prepared By/For

Representation

```
<metadata>
   <!-- prop -->
   <role id="role-document-by">
      <title>Prepared By</title>
      <desc>The organization that prepared this SSP.</desc>
   </role>
   <role id="role-document-for">
      <title>Prepared For</title>
      <desc>The organization for which this SSP was prepared.</desc>
   </role>
   <!-- cut -->
   <party id="csp">
      <org>
         <org-name>Cloud Service Provider (CSP) Name</org-name>
         <short-name>CSP Acronym/Short Name</short-name>
         <address>
            <!-- address lines cut here for space -->
         </address>
      </org>
   </party>
   <responsible-party role-id="role-ssp-by">
      <party-id>csp</party-id>
   </responsible-party>
   <responsible-party role-id="role-ssp-for">
      <party-id>csp</party-id>
   </responsible-party>
</metadata>
<!-- cut -->
<back-matter>
   <!-- citations -->
   <resource id="csp-logo">
      <desc>CSP Logo</desc>
      <rlink href="./logo.png" media-type="image/png" />
      <base64 filename='logo.png'>--- base64 content cut ---</base64>
   </resource>
</back-matter>
```

FedRAMP-Defined Identifiers
Required Role ID's:
- role-document-by
- role-document-for

FedRAMP-Defined Identifier
Required Party ID:
- party-csp

XPath Queries

```
CSP's Logo:
  /*/back-matter/resource[@id=csp-logo']/base64          OR
  /*/back-matter/resource[@id="csp-logo"]/rlink/@href

Prepared By Details:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='role-ssp-by']/party-
  id]]/org/org-name

Prepared For Details:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='role-ssp-for']/party-
  id]]/org/org-name

NOTE: Replace "org-name" with "addr-line", "city", "state", or "zip" as needed. There may be
  more than one addr-line.
```

NOTES:

- If this was prepared by a 3PAO, their logo should also be a resource in the back-matter with a resource ID of '3pao-logo', and that ID should be used here in place of 'csp-logo' for Prepared By.

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@FedRAMP.gov*

For more information about the FedRAMP project, see www.FedRAMP.gov

Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).

In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Note that "-1" Controls (AC-1, AU-1, SC-1, etc.)* cannot be inherited and must be described in some way by the service provider.
*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (IaaS) (or anything lower in the stack), the "inherited" check box must be checked and the implementation description must simply say "inherited." FedRAMP reviewers will determine whether the control-set is appropriate or not.

4.3. Document Revision History

Document revision history is not yet available in OSCAL. NIST expects to include it in Milestone Release 3 (MR-3).

This space is a placeholder and will be updated, once that feature is available.

4.4. How to Contact Us

The FedRAMP email and web site addresses are part of the organizational content for the FedRAMP PMO.

Representation

```
...<metadata>
      <!-- role -->
      <party id="party-fedramp-pmo">
         <org>
            <org-name>Federal Risk and Authorization Management Program: PMO</org-name>
            <short-name>FedRAMP PMO</short-name>
            <address>
               <addr-line>1800 F St. NW</addr-line>
               <city>Washington</city>
               <state>DC</state>
               <postal-code></postal-code>
               <country>us</country>
            </address>
            <email>info@fedramp.gov</email>
            <url>https://fedramp.gov</url>
         </org>
      </party>
      <!-- responsible-party -->
...<metadata>
```

FedRAMP-Defined Identifiers
Required Party IDs:
- party-fedramp-pmo
- party-fedramp-jab

XPath Queries

```
FedRAMP email address:
  /*/metadata/party[@id='party-fedramp-pmo']/org/email

FedRAMP web site:
  /*/metadata/party[@id='party-fedramp-pmo']/org/url
```

NOTE:

- None.

System Security Plan Approvals

Cloud Service Provider Signatures

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

Name	<Enter Name>	Date	<Select Date>
Title	<Enter Title>		
Cloud Service Provider	CSP Name		

4.5. System Security Plan Approvals

Representation

FedRAMP-Defined Identifier
Required Party ID:
- `role-document-approver`

```
<metadata>
   <!-- prop, link -->
   <role id="role-document-approver">
      <title>System Security Plan Approval</title>
      <desc>The individual or individuals within the CSP authorized to take
                                    responsibility for the accuracy of this SSP.</desc>
   </role>
   <!-- cut -->
   <party id="person-001">
      <person>
         <person-name>Name 1</person-name>
         <org-id>csp</org-id>
         <prop name="title" ns="fedramp">Individual's Title</prop>
      </person>
   </party>
   <party id="person-002">
      <person>
         <person-name>Name 2</person-name>
         <org-id>csp</org-id>
         <prop name="title" ns="fedramp">Individual's Title</prop>
      </person>
   </party>
   <!-- cut -->
   <responsible-party role-id="role-ssp-approver">
      <party-id>person-001</party-id>
      <party-id>person-002</party-id>
   </responsible-party>
   <!-- remarks (or nothing else under metadata) -->
</metadata>
```

FedRAMP Extension
Person's Title:
- `prop name="title" ns="fedramp"`

XPath Queries

```
Approver's Name:
  (/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='role-ssp-
  approver']/party-id]]/person/person-name)[1]

Approver's Title:
  (/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id='role-ssp-
  approver']/party-id]]/person/prop[@name='title'][@ns='fedramp'])[1]

NOTE: For each additional approver, replace the "[1]" with "[2]", "[3]", and so on.

CSP Name:
  /*/metadata/party[@id='csp']/org/org-name
```

NOTES:

- A person's title is not a valid OSCAL field. This uses a FedRAMP extension to capture a person's title.
- The code above shows two approvers. At least one is required. There is no limit to the number of approvers; however, FedRAMP encourages no more than three.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter Information System Abbreviation system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
<Enter FedRAMP Application Number>	Information System Name	Enter Information System Abbreviation

4.6. Information System Name, Title, and FedRAMP Identifier

The FedRAMP-assigned application number is the unique ID for a FedRAMP system. OSCAL supports several system identifiers, which may be assigned by different organizations.

For this reason, OSCAL requires the `identifier-type` flag be present and have a value that uniquely identifies the issuing organization. FedRAMP requires its value to be "`http://fedramp.gov`" for all FedRAMP-issued application numbers.

Representation

```
<system-characteristics>
   <system-id identifier-type="http://fedramp.gov">F00000000</system-id>
   <system-name>System's Full Name</system-name>
   <system-name-short>System's Short Name or Acronym</system-name-short>
   <!-- description -->
</system-characteristics>
```

FedRAMP-Defined Identifier

Required Identifier Type:

- `identifier-type="http://fedramp.gov"`

XPath Queries

```
FedRAMP System Identifier:
  /*/system-characteristics/system-id[@identifier-type="https://fedramp.gov"]

Information System Name:
  /*/system-characteristics/system-name

Information System Abbreviation:
  /*/system-characteristics/system-name-short
```

NOTE:

- None.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is recorded in Table 2-1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10. FIPS 199**.

Table 2-1. Security Categorization

System Sensitivity Level:	Choose level.

4.7. Information System Categorization and FedRAMP Baselines

Table 2-1 and Table 2-4 Representation

```
<system-characteristics>
   <!-- description -->
   <prop name="authorization-type" ns="fedramp">fedramp-agency</prop>
   <!-- annotation, link, date-authorized -->
   <security-sensitivity-level>moderate</security-sensitivity-level>
   <!-- system-information -->
</system-characteristics>
```

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp"`):

- `name="authorization-type"`
  - **Valid:** `fedramp-jab, fedramp-agency, fedramp-li-saas`

OSCAL Accepted Values

Valid values for `security-sensitivity-level`:

- `low`
- `moderate`
- `high`

XPath Queries

```
System Sensitivity Level:
  /*/system-characteristics/security-sensitivity-level

URL to OSCAL-based FedRAMP Baseline File:
  /*/import-profile/@href

FedRAMP Authorization Type:
  /*/system-characteristics/prop[@name="authorization-type"][@ns="fedramp"]
```

NOTES:

- The identified System Sensitivity Level governs which FedRAMP baseline applies. See Appendix A for more information about importing the appropriate FedRAMP baseline.

The `adjustment-justification` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.

Delete this instruction from your final version of this document.

Example:

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availabil
System Development	C.3.5.1	Low	Moderate	Low

Table 2-2. Sensitivity Categorization of Information Types

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.

FedRAMP Accepted Values
FedRAMP only accepts NIST SP 800-60 IDs. The `system` flag of the `information-type-id` field must be:

- `nist`

OSCAL Accepted Values
Valid impact (base/selected) values:

- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

4.8. Information Types

Table 2-2 and Table 15-9 Representation

```
<system-information>
   <!-- security-sensitivity-level -->
   <information-type name="Information Type Name" id="info-01">
      <information-type-id system="nist">C.2.4.1</information-type-id>
      <confidentiality-impact>
         <base>fips-199-moderate</base>
         <selected>fips-199-moderate</selected>
         <adjustment-justification><p>Description</p></adjustment-justification>
      </confidentiality-impact>
      <integrity-impact>
         <base>fips-199-moderate</base>
         <selected>fips-199-moderate</selected>
         <adjustment-justification><p>Description</p></adjustment-justification>
      </integrity-impact>
      <availability-impact>
         <base>fips-199-moderate</base>
         <selected>fips-199-moderate</selected>
         <adjustment-justification><p>Description</p></adjustment-justification>
      </availability-impact>
   </information-type>
   <!-repeat the information-type assembly for each information type -->
   <!-- security-impact-levels -->
</system-information>
```

NOTES:

- Table 2-2 is a subset of Table 15-9. The above OSCAL representation satisfies both.
- For each impact type, if the `selected` field does not match the `base` field, the `adjustment-justification` field is required.

Table 2-2 is a sub-set of Table 15-9 as follows:

Table Column	Table 2-2	Table 15-9	XPath Queries
Information Type	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/@name`
NIST 800-60 Identifier	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/information-type-id[@system="nist"]`
NIST Recommended Confidentiality Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/base`
NIST Recommended Integrity Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/integrity-impact/base`
NIST Recommended Availability Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/availability-impact/base`
CSP Selected Confidentiality Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/selected`
CSP Selected Integrity Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/integrity-impact/selected`
CSP Selected Availability Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/availability-impact/selected`

Impact Adjustment Justification	No	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/adjustment-justification/`
			`//system-characteristics/system-information/information-type[1]/integrity-impact/adjustment-justification/`
			`//system-characteristics/system-information/information-type[1]/availability-impact/adjustment-justification/`

In each XPath query in the table above, replace the "[1]" with "[2]", "[3]", as needed, up to the number of information-type fields that exist in the file.

Use the following XPath statement to count the number of information-type fields: `count(//system-characteristics/system-information/information-type)`

The FedRAMP SSP Template has only one table cell for the justification of changing any of the three recommended NIST 800-60 levels. OSCAL ties this justification to its individual type (confidentiality, availability, or integrity). If recreating Table 15-9, display all three justifications in this field if present, and label the.

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2-3. Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Choose level.
Integrity	Choose level.
Availability	Choose level.

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2-4. Baseline Security Configuration that follows.

Table 2-4. Baseline Security Configuration

Enter Information System Abbreviation Security Categorization	Choose level

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

4.9. Security Objectives Categorization (FIPS 199)

Representation

```
<system-characteristics>
   <!-- cut -->
   <security-sensitivity-level>moderate</security-sensitivity-level>
   <!-- system-information -->




   <security-impact-level>
      <security-objective-confidentiality>fips-199-moderate
         </security-objective-confidentiality>

      <security-objective-integrity>fips-199-moderate</security-objective-integrity>
      <security-objective-availability>fips-199-moderate

         </security-objective-availability>
   </security-impact-level>
   <!-- status -->
</system-characteristics>
```

OSCAL Accepted Values
Valid security sensitivity values:
- `low`
- `moderate`
- `high`

OSCAL Accepted Values
Valid security objective values:
- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

XPath Queries

```
System Sensitivity Level:
  /*/system-characteristics/security-sensitivity-level


Security Objective: Confidentiality:
  /*/system-characteristics/security-impact-level/security-objective-confidentiality
Security Objective: Integrity:
  /*/system-characteristics/security-impact-level/security-objective-integrity
Security Objective: Availability:
  /*/system-characteristics/security-impact-level/security-objective-availability
```

NOTES:

- The `security-sensitivity-level` field in the OSCAL file satisfies both Table 2-1 and 2-4.
- The only valid values for the `security-objective-confidentiality`, `security-objective-integrity`, and `security-objective-availability` fields are: `"fips-199-low"`, `"fips-199-moderate"`, and `"fips-199-high"`.
- The only valid values for the `security-sensitivity-level` field are: `"low"`, `"moderate"`, and `"high"`.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

2.3. Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

4.10. Digital Identity Determination

The digital identity level identified in Section 2.3 is the same as the level in Attachment 3. Both are identified with the same single piece of information, which is a `prop` field with the `name` "`security-eauth-level` ".

This is a FedRAMP extension, thus requires the `ns` flag set to "`fedramp`".

Currently, FedRAMP prescribes an overall eAuth level, and does not require individual IAL, AAL, and FAL designations. The overall eAuth level is all that is required; however, the FedRAMP extensions include separate prop statements for each of these three levels to allow for possible future use.

Representation

```
<system-characteristics>

   <prop name="security-eauth-level" class="security-eauth" ns="fedramp">moderate</prop>

   <!-- Attachment 3, Digital Identity Worksheet -->
   <prop name="security-eauth-ial" class="security-eauth" ns="fedramp">moderate</prop>
   <prop name="security-eauth-aal" class="security-eauth" ns="fedramp">moderate</prop>
   <prop name="security-eauth-fal" class="security-eauth" ns="fedramp">moderate</prop>
</system-characteristics>
```

FedRAMP Extensions

prop:

- `name="security-eauth-level" ns="fedramp"`
- `name="security-eauth-ial" ns="fedramp"`
- `name="security-eauth-aal" ns="fedramp"`
- `name="security-eauth-fal" ns="fedramp"`

FedRAMP Accepted Values

Valid eAuth values:

- `low`
- `moderate`
- `high`

XPath Queries

```
Digital Identity Level:
  /*/system-characteristics/prop[@name="security-eauth-level"][@ns='fedramp']

Identity Assurance Level:
  /*/system-characteristics/prop[@name="security-eauth-ial"][@ns='fedramp']

Authenticator Assurance Level:
  /*/system-characteristics/prop[@name="security-eauth-aal"][@ns='fedramp']

Federation Assurance Level:
  /*/system-characteristics/prop[@name="security-eauth-fal"][@ns='fedramp']
```

NOTE:

- None.

3. INFORMATION SYSTEM OWNER

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Information System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4.11. Information System Owner

Representation

```
   <metadata>
      <!-- cut -->
      <role id="role-system-owner">
         <title>Information System Owner</title>
         <desc>The individual within the CSP who is ultimately accountable for
everything related to this system.</desc>
      </role>
      <!-- cut -->
      <party id="person-001">
         <person>
            <person-name>Name of Person 1</person-name>
            <org-id>csp</org-id>
            <address>
               <addr-line></addr-line>
               <city>City</city>
               <state>ST</state>
               <postal-code>12345</postal-code>
               <country>US</country>
            </address>
            <email>name@org.domain</email>
            <phone></phone>
            <prop name="title" ns="fedramp">Individual's Title</prop>
         </person>
      </party>
      <!-- cut -->
      <responsible-party role-id=" role-system-owner ">
         <party-id>person-001</party-id>
      </responsible-party>
   </metadata>
```

FedRAMP-Defined Identifier
Required role ID:
- `role-system-owner`

XPath Queries

System Owner's Name:
```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-
owner"]/party-id]]/person/person-name
```

NOTE: Replace "person-name" with "org-name", "email" or "phone" above as needed.

System Owner's Address:
```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-
owner"]/party-id]]/person/address/addr-line
```

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

System Owner's Title:
```
/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-
owner"]/party-id]]/person/prop[@name='title'][@ns='fedramp']
```

Company/Organization:
```
/*/metadata/party[@id=((/*/metadata/party[@id=[/*/metadata/responsible-party[@role-
id="role-system-owner"]/party-id]]/person/org-id)[1])]/org/org-name
```

NOTE:

- If no country is provided, FedRAMP tools will assume a US address.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

4. AUTHORIZING OFFICIALS

Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.

JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)

Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information

Delete this and all other instructions from your final version of this document.

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the ***Insert AO information as instructed above***.

FedRAMP JAB P-ATO Authorization Representation

```
   <metadata>
      <!-- cut -->
      <role id="role-system-ao">
         <title>Authorizing Official</title>
         <desc>The individual or individuals who must grant this system an
authorization to operate.</desc>
      </role>
      <!-- cut -->
      <party id="fedramp-jab">
         <org>
            <org-name>Federal Risk and Authorization Management Program: Joint
Authorization Board</org-name>
            <short-name>FedRAMP JAB</short-name>
         </org>
      </party>
      <!-- cut -->
      <responsible-party role-id=" role-system-ao ">
         <party-id>fedramp-jab</party-id>
      </responsible-party>
   </metadata>
   <!-- import -->

   <system-characteristics>
   <!-- description -->
      <prop name="authorization-type" ns="fedramp">fedramp-jab</prop>
   <!-- annotation -->
   </system-characteristics>
```

JAB XPath Queries

```
Authorizing Official's Name:
  //metadata/party[@id=[//metadata/responsible-party[@role-id="role-system-
  ao"]/party-id]]/org/short-name
```

4.12. Authorizing Officials

FedRAMP Agency Authorization Representation

```
   <metadata>
      <!-- cut -->
      <role id="role-system-ao">
         <title>Authorizing Official</title>
         <desc>The individual or individuals who must grant this system an authorization
to operate.</desc>
      </role>
      <!-- cut -->
      <party id="person-003">
         <person>
            <person-name>Name of Person 1</person-name>
            <org-name>A Four Letter Agency</org-name>
            <address>
               <addr-line></addr-line>
               <city></city>
               <state></state>
               <postal-code></postal-code>
               <country>us</country>
            </address>
            <prop name="title" ns="fedramp">Individual's Title</prop>
         </person>
      </party>
      <!-- cut -->
      <responsible-party role-id=" role-system-ao ">
         <party-id>person-003</party-id>
      </responsible-party>
   </metadata>

   <!-- import -->

   <system-characteristics>
   <!-- description -->
      <prop name="authorization-type" ns="fedramp">fedramp-agency</prop>
   <!-- annotation -->
   </system-characteristics>
```

FedRAMP-Defined Identifier
Required Role ID:
- `role-system-ao`

FedRAMP Extension
Authorization Type:
- `prop name="authorization-type" ns="fedramp"`

FedRAMP Accepted Values
- `fedramp-jab`
- `fedramp-agency`
- `fedramp-li-saas`

Authorization Type XPath Query

```
FedRAMP Authorization Type:
  /*/system-characteristics/prop[@name="authorization-type"][@ns="fedramp"]
```

FedRAMP Agency and LI-SaaS XPath Queries

```
Authorizing Official's Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-ao"]/party-
  id]]/person/person-name

Authorizing Official's Title:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-ao"]/party-
  id]]/person/prop[@name='title'][@ns='fedramp']

Authorizing Official's Agency:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-ao"]/party-
  id]]/person/org-name
```

NOTE:

- if the `authorization-type` field is "`fedramp-jab`", the `responsible-party/party-id` field must be "`fedramp-jab`", and vice versa.

5. OTHER DESIGNATED CONTACTS

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Next Page

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>

4.13. Other Designated Contacts: Information System Management

Table 5-1 Representation

```
   <metadata>
      <!-- cut -->
      <role id="role-system-poc-manager">
         <title>Information System Management Point of Contact (POC)</title>
         <desc>The highest level manager who responsible for system operation on behalf of the
System Owner.</desc>
      </role>
      <!-- cut -->
      <party id="person-005">
         <person>
            <person-name>Name 5</person-name>
            <org-name>csp</org-name>
            <address>
               <addr-line>Address Line</addr-line>
               <city>City</city>
               <state>ST</state>
               <postal-code>00000</postal-code>
               <country>US</country>
            </address>
            <email>name@org.domain</email>
            <phone></phone>
            <prop name="title" ns="fedramp">Individual's Title</prop>
         </person>
      </party>
      <!-- cut -->
      <responsible-party role-id="role-system-poc-manager">
         <party-id>person-005</party-id>
      </responsible-party>
      <responsible-party role-id="role-system-poc-technical">
         <party-id>person-006</party-id>
      </responsible-party>
   </metadata>
```

FedRAMP-Defined Identifiers
Required Role ID's:
- `role-system-poc-manager`
- `role-system-poc-technical`

FedRAMP Extension
Person's Title:
- `prop name="title" ns="fedramp"`

XPath Queries

```
Information System Management POC Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/person-name

NOTE: Replace "person-name" with "email" or "phone" above as needed.

Information System Management POC Title:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/prop[@name='title'][@ns="fedramp"]

Information System Management POC Address Line:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.
```

NOTES:

None.

5. OTHER DESIGNATED CONTACTS

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Previous Page

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>

4.14. Other Designated Contacts: Information System Technical

Table 5-2 Representation

```
   <metadata>
      <!-- cut -->
      </role>
      <role id="role-system-poc-technical">
         <title>Information System Technical Point of Contact</title>
         <desc>The individual or individuals leading the technical operation of the
system.</desc>
      </role>
      <party id="person-007">
         <person>
            <person-name>Name 7</person-name>
            <org-name>csp</org-name>
            <address>
               <addr-line>Address Line</addr-line>
               <city>City</city>
               <state>ST</state>
               <postal-code>00000</postal-code>
               <country>US</country>
            </address>
            <email>name@org.domain</email>
            <phone></phone>
            <prop name="title" ns="fedramp">Individual's Title</prop>
         </person>
      </party>
      <!-- repeat party assembly for each person -->
      <!-- cut -->
      <responsible-party role-id="role-system-poc-technical">
         <party-id>person-007</party-id>
         <party-id>person-008</party-id>
         <party-id>person-009</party-id>
      </responsible-party>
   </metadata>
```

FedRAMP-Defined Identifier
Required Role ID:
- `role-system-poc-technical`

FedRAMP Extension
Person's Title:
- `prop name="title" ns="fedramp"`

XPath Queries

```
Information System Technical POC Name:
  (/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  technical"]/party-id]]/person/person-name)[1]

NOTE: Replace "person-name" with "email" or "phone" above as needed.

Information System Technical POC Title:
  (/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  technical"]/party-id]]/person/prop[@name='title'][@ns="fedramp"])[1]

Information System Technical POC Address Line:
  (/*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  technical"]/party-id]]/person/address/addr-line)[1]

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

NOTE: For each additional technical POC, replace the "[1]" with "[2]", "[3]", and so on.
```

NOTES:

- None.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Next Page

4.15. Assignment of Security Responsibility: ISSO

Table 6-1 Representation

```
   <metadata>
      <!-- cut -->
      <role id="role-system-isso">
         <title>System Information System Security Officer (or Equivalent)</title>
         <desc>The individual accountable for the security posture of the system on behalf of
the system owner.</desc>
      </role>
      <!-- cut -->
      <party id="person-010">
         <person>
            <person-name>Name 10</person-name>
            <org-name>CSP Name</org-name>
            <address>
               <addr-line>Address Line</addr-line>
               <city>City</city>
               <state>ST</state>
               <postal-code>00000</postal-code>
               <country>US</country>
            </address>
            <email>name@org.domain</email>
            <phone></phone>
            <prop name="title" ns="fedramp">Individual's Title</prop>
         </person>
      </party>
      <!-- cut -->
      <responsible-party role-id="role-system-isso">
         <party-id>person-010</party-id>
      </responsible-party>
   </metadata>
```

FedRAMP-Defined Identifiers
Required Role ID:
- `role-system-isso`

FedRAMP Extension
Person's Title:
- `prop name="title" ns="fedramp"`

XPath Queries

```
Information System Management POC Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/person-name

NOTE: Replace "person-name" with "org-name", "email", or "phone" above as needed.

Information System Management POC Title:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/prop[@name='title'][@ns="fedramp"]

Information System Management POC Address Line:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.
```

NOTE:

- None.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Previous Page

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4.16. Assignment of Security Responsibility: AO POC

Table 6-2 Representation

```
<metadata>
   <!-- cut -->
   <role id="role-system-ao-poc">
      <title>Authorizing Official's Point of Contact</title>
      <desc>The individual representing the authorizing official.</desc>
   </role>
   <!-- cut -->
   <party id="person-011">
      <person>
         <person-name>Name 11</person-name>
         <org-name>Agency Name</org-name>
         <address>
            <addr-line>Address Line</addr-line>
            <city>City</city>
            <state>ST</state>
            <postal-code>00000</postal-code>
            <country>US</country>
         </address>
         <email>name@org.domain</email>
         <phone></phone>
         <prop name="title" ns="fedramp">Individual's Title</prop>
      </person>
   </party>
   <!-- cut -->
   <responsible-party role-id="role-system-ao-poc">
      <party-id>person-011</party-id>
   </responsible-party>
</metadata>
```

FedRAMP-Defined Identifier
Required Role ID:
- `role-system-ao-poc`

FedRAMP Extension
Person's Title:
- `prop name="title" ns="fedramp"`

XPath Queries

```
Information System Management POC Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/person-name

NOTE: Replace "person-name" with "email" or "phone" above as needed.

Information System Management POC Title:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/prop[@name='title'][@ns="fedramp"]

Information System Management POC Address Line:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-poc-
  manager"]/party-id]]/person/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.
```

NOTE:

- None.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase shown in Table 7-1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7-1. System Status

System Status		
☐	Operational	The system is operating and in production.
☐	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Other	Explain: Click here to enter text.

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

Delete this and all other instructions from your final version of this document.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.17. Information System Operational Status

Representation

```
   <system-characteristics>
      <!-- cut -->

      <!-- security-impact-level -->
      <status state="operational">
         <remarks><p>Remarks are required if status/state is "other". Optional
otherwise.</p></remarks>
      </status>
      <!-- leveraged-authorization -->




      <!-- cut -->
   </system-characteristics>
```

OSCAL Accepted Values

Valid state values:

- `operational`
- `under-development`
- `under-major-modification`
- `disposition`
- `other`

XPath Queries

```
System's Operational Status:
  /*/system-characteristics/status/@state

The number of paragraphs in the Operational Status Remarks:
  count(/*/system-characteristics/status/remarks/p[1])

Remarks on System's Operational Status:
  /*/system-characteristics/status/remarks
```

NOTE:

- If the status is "`other`", the `remarks` field is required. Otherwise it is optional.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	**Explain:** Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.18. Cloud Service Models

Representation

```
<system-characteristics>
   <!-- cut -->



   <!-- prop -->
   <annotation name="service-model" ns="fedramp" value="saas">
      <remarks>
         <p>Remarks are required if service model is "other". Optional otherwise.</p>
      </remarks>
   </annotation>
   <!-- link or date authorized -->



   <!-- cut -->
</system-characteristics>
```

FedRAMP Extension
annotation:
- `name="service-model" ns="fedramp"`

FedRAMP Accepted Values
Valid Service Model values:
- `saas`
- `paas`
- `iaas`
- `other`

XPath Queries

```
Service Model:
  /*/system-characteristics/annotation[@name="service-model"][@ns="fedramp"]/@value

Remarks on System's Service Model:
  /*/system-characteristics/annotation[@name="service-model"][@ns="fedramp"]/remarks
```

NOTE:

- If the service model is "`other`", the `remarks` field is required. Otherwise it is optional.

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
☐	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
☐	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
☐	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.19. Cloud Deployment Models

Representation

```
<system-characteristics>
   <!-- cut -->


   <!-- prop -->
   <annotation name="deployment-model" ns="fedramp" value="public">
      <remarks>
         <p>Remarks are required if deployment model is "hybrid". Optional otherwise.</p>
      </remarks>
   </annotation>
   <!-- link or date authorized -->


   <!-- cut -->
</system-characteristics>
```

FedRAMP Extension
annotation:
- `name="deployment-model" ns="fedramp"`

FedRAMP Accepted Values
Valid Service Model values:
- `public`
- `private`
- `community-usgov-only`
- `hybrid`

XPath Queries

```
Deployment Model:
  /*/system-characteristics/annotation[@name="deployment-model"][@ns="fedramp"]/@value

Remarks on System's Deployment Model:
  /*/system-characteristics/annotation[@name="deployment-model"][@ns="fedramp"]/remarks
```

NOTE:

- If the deployment model is "`hybrid`", the `remarks` field is required. Otherwise it is optional.

8.3. Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer's Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write "None" in the first column of the table that follows. cAdd as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The Enter Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Enter Information System Abbreviation are listed in Table 8-3. Leveraged Authorizations that follows.

Table 8-3. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

At the time of writing, the NIST OSCAL syntax validation tools require the `leveraged-authorization` `@name` attribute, and limits the value to NCName type. This section will be updated when the issue is closed by NIST as tracked HERE.

4.20. Leveraged Authorizations

Representation

```
   <metadata>
      <!-- role -->
      <party id="party-bip">
         <org>
            <org-name>Big IaaS Provider</org-name>
            <short-name>B.I.P.</short-name>
            <remarks>
               <p>Underlying service provider. Leveraged Authorization.</p>
            </remarks>
         </org>
      </party>
      <!-- responsible-party -->
   </metadata>
   <!-- cut -->
   <system-characteristics>
      <!-- status -->
      <leveraged-authorization id="lva-1" name="NCName">
         <annotation name="system-name" id="leveraged-01-name" ns="fedramp" value="MegaIaaS">
            <remarks><p>Remarks about this system</p></remarks>
         </annotation>
         <party-id>party-bip</party-id>
         <date-authorized>2018-11-27</date-authorized>
         <remarks><p>Overall notes about the inheritance of controls from this
system</p></remarks>
      </leveraged-authorization>
      <!-- Repeat leveraged-authorization assembly for each leveraged authorization -->
      <!-- authorization-boundary -->
   </system-characteristics>
```

FedRAMP Extension
annotation:
- `name="system-name" ns="fedramp"`

XPath Queries

```
Leveraged Authorization System Name:
  /*/system-characteristics/leveraged-authorization[1]/annotation[@name="system-
  name"][@ns="fedramp"]/@value

Leveraged Authorization Remarks:
  /*/system-characteristics/leveraged-authorization[1]/annotation[@name="system-
  name"][@ns="fedramp"]/remarks

Leveraged Service Provider Owner:
  /*/metadata/party[@id=/*/system-characteristics/leveraged-authorization[1]/party-
  id]/org/org-name

Date Granted:
  /*/system-characteristics/leveraged-authorization[1]/date-authorized
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- The `id` for `leveraged-authorization` is required by FedRAMP, even though it is optional in the OSCAL syntax. The `id` will be used by each control that inherits from this system.
- If more than one leveraged authorization exists for the system, repeat the entire assembly for each leveraged authorization. Currently this is not typical and should be discussed in advance with the FedRAMP PMO.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.1. System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

Delete this and all other instructions from your final version of this document.

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.21. System Function or Purpose

Representation

```
<system-characteristics>
   <!-- system-name, system-name-short -->
   <description>
      <p>Describe the purpose and functions of this system here.</p>
   </description>
   <!-- prop, annotation, link, date-authorized -->
</system-characteristics>
```

XPath Query

```
System Function or Purpose: First paragraph in description
  /*/system-characteristics/description
```

NOTE:

- None.

9.2. Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system's Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

Additional FedRAMP Requirements and Guidance:

Guidance: *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1. Authorization Boundary Diagram below.

Figure 9-1. Authorization Boundary Diagram

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.22. Authorization Boundary Diagram

The OSCAL approach to this type of diagram is to treat the image data as either a linked or base64-encoded resource in the back-matter section of the OSCAL file, then use a reference to the diagram within the body of the OSCAL file.

Representation

```
<system-characteristics>
   <!-- leveraged-authorization -->
   <authorization-boundary>
      <description>
         <p>A holistic, top-level explanation of the FedRAMP authorization boundary.</p>
      </description>
      <diagram id="sys-boundary-1">
         <description><p>A diagram-specific explanation.</p></description>
         <link href="#diag-boundary-1"/>
         <caption>Authorization Boundary Diagram</caption>
      </diagram>
      <!-- repeat diagram assembly for each additional boundary diagram -->
   </authorization-boundary>
   <!-- network-architecture -->
</system-characteristics>


<!-- cut -->


<back-matter>
   <!-- citation -->
   <resource id="diag-boundary-1">
      <desc>The primary authorization boundary diagram.</desc>
      <base64>00000000</base64>
   </resource>
</back-matter>
```

FedRAMP-Defined Identifiers
Diagram ID:
- `sys-boundary-1`

Resource ID:
- `diag-boundary-1`

Replace **1** with a number (2, 3, etc.) as needed. There should always be a -1 in a SSP.

XPath Queries

```
Overall Description:
  /*/system-characteristics/authorization-boundary/description

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/authorization-boundary/diagram)

Link to First Diagram:
  /*/system-characteristics/authorization-boundary/diagram[1]/link/@href

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@id=""]/base64
  OR:
  /*/back-matter/resource[@id=""]/rlink/@href

First Diagram Description:
  /*/system-characteristics/authorization-boundary/diagram[@id="authorization-boundary-
  1"]/description
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- While resources may generally be linked or embedded, FedRAMP *prefers* the authorization boundary diagram to be embedded (base64).

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

Instruction: For an External User, write "Not Applicable" in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

See Next Page

4.23. Personnel Roles and Privileges

Representation

```
<metadata>
   <role id="role-admin-unix">
      <title>Unix Administrator</title>
      <desc>This is a sample role.</desc>
   </role>
</metadata>
<!-- import -->
<!-- system characteristics -->
<system-implementation>
   <!-- prop -->
   <user id="sys-role-1">
      <title>Unix System Administrator</title>
      <prop name="user-type" ns="fedramp">external</prop>
      <prop name="privilege-type" ns="fedramp">NLA</prop>
      <prop name="sensitivity-level" ns="fedramp">limited</prop>
      <role-id>role-admin-unix</role-id>
      <authorized-privilege name="Full administrative access (root)">
         <function-performed>Add/remove users and hardware</function-performed>
         <function-performed>install and configure software</function-performed>
         <function-performed>OS updates, patches and hotfixes</function-performed>
         <function-performed>perform backups</function-performed>
      </authorized-privilege>
   </user>
   <!-- repeat user assembly for each row in Table 9-1 -->
</system-implementation >
```

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp"`):

- `name="user-type"`
  - **Valid:** `internal, external`
- `name="privilege-type"`
  - **Valid:** `P, NP, NLA`
- `name="sensitivity-level"`
  - **Valid:** `high-risk, severe, moderate, limited, na`

XPath Queries

```
Number of entries in the role table:
  count(/*/system-implementation/user)

Role:
  /*/system-implementation/user[1]/title

Internal or External:
  /*/system-implementation/user[1]/prop[@name="user-type"][@ns="fedramp"]

Privileged, Non-Privileged, or No Logical Access:
  /*/system-implementation/user[1]/prop[@name="privilege-type"][@ns="fedramp"]

Sensitivity Level:
  /*/system-implementation/user[1]/prop[@name="sensitivity"][@ns="fedramp"]

Authorized Privileges:
  /*/system-implementation/user[1]/authorized-privilege/@name[1]
  count(/*/system-implementation/user[1]/authorized-privilege)

Functions Performed:
  /*/system-implementation/user[1]/authorized-privilege[1]/function-performed[1]
  count(/*/system-implementation/user[1]/authorized-privilege[1]/function-performed)
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- FedRAMP prefers separate `function-performed` fields for each function performed but will accept all functions in one field.
- The `authorized-privilege` field should also be duplicated within a user assembly if there is more than one.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

Instruction: For an External User, write "Not Applicable" in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

See Previous Page

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

4.24. Number of Users

Representation

```
<system-implementation>
   <prop name="users-internal" ns="fedramp">22</prop>
   <prop name="users-external" ns="fedramp">110</prop>
   <prop name="users-internal-future" ns="fedramp">25</prop>
   <prop name="users-external-future" ns="fedramp">200</prop>
</system-implementation>
```

FedRAMP Extensions

prop (`ns="fedramp"`):

- `name="users-internal"`
- `name="users-external"`
- `name="users-internal-future"`
- `name="users-external-future"`

XPath Queries

```
Number of current internal users:
  /*/system-implementation/prop[@name="users-internal"][@ns="fedramp"]

Number of current external users:
  /*/system-implementation/prop[@name="users-external"][@ns="fedramp"]

Number of future internal users (1 year):
  /*/system-implementation/prop[@name="users-internal-future"][@ns="fedramp"]

Number of future external users (1 year):
  /*/system-implementation/prop[@name="users-external-future"][@ns="fedramp"]
```

NOTE:

- None.

9.4. Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9-2. Network Diagram mapping the data flow between components.

The following Figure 9-2. Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

Figure 9-2. Network Diagram

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.25. Network Architecture Diagram(s)

Representation

```
<system-characteristics>
   <!-- authorization-boundary -->
   <network-architecture>
      <description>
         <p>A holistic, top-level explanation of the system's network.</p>
      </description>
      <diagram id=" sys-network-1">
         <description><p>A diagram-specific explanation.</p></description>
         <link href="#diag-network-1"/>
         <caption>Network Diagram</caption>
      </diagram>
      <!-- repeat diagram assembly for each additional network diagram -->
   </network-architecture>
   <!-- data-flow -->
</system-characteristics>


<!-- cut -->


<back-matter>
   <!-- citation -->
   <resource id="diag-network-1">
      <desc>The primary network diagram.</desc>
      <rlink href="./diagram.jpg" media-type="image/jpeg"/>
   </resource>
</back-matter>
```

FedRAMP-Defined Identifiers
Diagram ID:
- `sys-network-1`

Resource ID:
- `diag-network-1`

Replace **1** with a number (2, 3, etc.) as needed. There should always be a -1 in a SSP.

XPath Queries

```
Overall Description:
  /*/system-characteristics/network-architecture/description

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/network-architecture/diagram)

Link to First Diagram:
  /*/system-characteristics/network-architecture/diagram[1]/link/@href

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@id=""]/base64
  OR:
  /*/back-matter/resource[@id=""]/rlink/@href

First Diagram Description:
  /*/system-characteristics/network-architecture/diagram[@id="sys-network-1"]/description
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the network architecture diagrams to be embedded (base64).

10.1. Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10-1. Data Flow Diagram, below.

Figure 10-1. Data Flow Diagram

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

4.26. Data Flow Diagrams

Representation

```
<system-characteristics>
   <!-- network-architecture -->
   <data-flow>
      <description>
         <p>A holistic, top-level explanation of the system's data flows.</p>
      </description>
      <diagram id="sys-dataflow-1">
         <description><p>A diagram-specific explanation.</p></description>
         <link href="#diag-dataflow-1"/>
         <caption>Data Flow Diagram</caption>
      </diagram>
      <!-- repeat diagram assembly for each additional data flow diagram -->
   </data-flow>
   <!-- network-architecture -->
</system-characteristics>


<!-- cut -->


<back-matter>
   <!-- citation -->
   <resource id="diag-dataflow-1">
      <desc>The primary data flow diagram.</desc>
      <base64>0000<!-- base64 cut -->0000</base64>
   </resource>
</back-matter>
```

FedRAMP-Defined Identifiers

Diagram ID:

- `sys-dataflow-1`

Resource ID:

- `diag-dataflow-1`

Replace **1** with a number (2, 3, etc.) as needed. There should always be a -1 in a SSP.

XPath Queries

```
Overall Description:
  /*/system-characteristics/data-flow/description

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/data-flow/diagram)

Link to First Diagram:
  /*/system-characteristics/data-flow/diagram[1]/link/@href

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@id=""]/base64
  OR:
  /*/back-matter/resource[@id=""]/rlink/@href

First Diagram Description:
  /*/system-characteristics/data-flow/diagram[@id="sys-dataflow-1"]/description
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the data flow diagrams to be embedded (base64).

10.2. Ports, Protocols and Services

The Table 10-1. Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled "Used By" please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled "Purpose" indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table 10-1. Ports, Protocols and Services

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

At the time of writing, the NIST OSCAL syntax validation tools treat the `service` `@name` attribute as and NCName datatype, instead of a string datatype. NIST is investigating. This section will be updated when the issue is closed by NIST as tracked HERE.

4.27. Ports, Protocols and Services

Representation

```
<system-implementation>
   <!-- component -->
   <service id="svc-1" name="ServiceName">
      <prop name="title" ns="fedramp">[SAMPLE]Service Name</prop>
      <prop name="used-by" ns="fedramp">What uses this service?</prop>
      <protocol name="http">
         <port-range start="80" end="80" transport="TCP"/>
      </protocol>
      <protocol name="https">
         <port-range start="443" end="443" transport="TCP"/>
      </protocol>
      <purpose>Describe the purpose of this service</purpose>
   </service>
   <!-- Repeat the service assembly for each row in Table 10-1 -->
   <!-- interconnection, system-inventory -->
</system-implementation>
```

FedRAMP Extensions

prop (`ns="fedramp"`):

- `name="title"`
- `name="used-by"`

XPath Queries

```
Number of entries in the Ports, Protocols and Services table:
  count(/*/system-implementation/service)

Number of protocols specified (1st service):
  count(/*/system-implementation/service[1]/protocol)

Number of port ranges specified:
  count(/*/system-implementation/service[1]/protocol[1]/port-range)

Ports: Start (1st service, 1st protocol, 1st port range):
  /*/system-implementation/service[1]/protocol[1]/port-range[1]/@start

Ports: End (1st service, 1st protocol, 1st port range):
  /*/system-implementation/service[1]/protocol[1]/port-range[1]/@end

Ports: Transport (1st service, 1st protocol, 1st port range):
  /*/system-implementation/service[1]/protocol[1]/port-range[1]/@transport

Protocol (1st service, 1st protocol):
  /*/system-implementation/service[1]/protocol[1]/@name

Service (1st service):
  /*/system-implementation/service[1]/prop[@name="title"][@ns="fedramp"]
  OR
  /*/system-implementation/service[1]/@name

Purpose (1st service):
  /*/system-implementation/service[1]/description

Used By (1st service):
  /*/system-implementation/service[1]/prop[@name="used-by"][@ns="fedramp"]
```

4.28. System Interconnections and Authorized Connections (Representation)

Table 11-1 and Table 13-3 are closely related and modeled together in OSCAL.

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

CSP Name | Information System Name   Version #.#, Date

11. SYSTEM INTERCONNECTIONS

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security, indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.

Additional FedRAMP Requirements and Guidance:

***Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

Table 11-1. System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

Representation

```
<metadata>
   <!-- oscal-version, prop -->
   <role id="role-ica-1">
      <title>Remote System POC</title>
      <desc>Role of person who signed the ICA.</desc>
   </role>
   <!-- repeat role assembly for each ICA -->
   <party id="party-ica-1">
      <person>
         <person-name>[SAMPLE]ICA POC's Name</person-name>
         <org-name>[SAMPLE]Remote Org Name</org-name>
         <email>person@ica.org.example</email>
         <phone>202-555-1212</phone>
      </person>
   </party>
   <!-- repeat party assembly for each ICA -->
</metadata>
<!-- import-profile, system-characteristics -->
   <interconnection id="ica-1">
      <remote-system-name>[EXAMPLE]Authorized Connection System Name</remote-system-name>
      <prop name="service-processor" ns="fedramp">[SAMPLE]Telco Name</prop>
      <prop name="ip-address-local" ns="fedramp">10.1.1.1</prop>
      <prop name="ip-address-remote" ns="fedramp">10.2.2.2</prop>
      <prop name="direction" ns="fedramp">incoming</prop>
      <prop name="information" ns="fedramp">string</prop>
      <prop name="port" ns="fedramp">string</prop>
      <prop name="circuit" ns="fedramp">string</prop>
      <annotation name="connection-security" ns="fedramp" value="ipsec">
         <remarks><p>If "other", remarks are required. Optional otherwise.</p></remarks>
      </annotation>
      <responsible-party role-id="role-ica-1">
         <party-id>party-ica-1</party-id>
      </responsible-party>
      <remarks><p>Optional notes about this interconnection</p></remarks>
   </interconnection>
   <!-- repeat interconnection assembly for each ICA -->
<!-- control-implementation -->
<back-matter>
   <citation id="cit-isa-1">
      <title>[SAMPLE]Interconnection Security Agreement Title</title>
      <prop name="publication" ns="fedramp">Document Version</prop>
   </citation>
   <!-- repeat citation assembly for each ICA -->
   <!-- resource -->
<back-matter>
```

FedRAMP Extensions & Accepted Values

prop (ns="fedramp"):
- name="service-processor"
- name="ip-address-local"
- name="ip-address-remote"
- name="direction"
  - **Valid:** incoming, outgoing
- name="information"
- name="port"
- name="circuit"

annotation (ns="fedramp"):
- name="connection-security"
  - **Valid:** ipsec, vpn, ssl, certificate, secure-file-transfer, other

FedRAMP Extension

prop (ns="fedramp"):
- name="publication"

XPath Queries

SEE NEXT PAGE

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

CSP Name | Information System Name Version #.#, Date

11. SYSTEM INTERCONNECTIONS

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security, indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.

Additional FedRAMP Requirements and Guidance:

Guidance: *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

Table 11-1. System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

4.29. System Interconnections and Authorized Connections (Queries)

Tables 11-1 and 13-3 are closely related and modeled together in OSCAL.

XPath Queries

Replace "[1]" with "[2]", "[3]", etc.

```
(11-1) Service Processor (SP):
  /*/system-implementation/interconnection[1]/prop[@name="service-processor"][@ns="fedramp"]
(11-1) IP Address and Interface:
  /*/system-implementation/interconnection[1]/prop[@name="ip-address-local"][@ns="fedramp"]
(11-1) External Organization Name ...:
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//org-name
  AND IP Address of System:
  /*/system-implementation/interconnection[1]/prop[@name="ip-address-remote"][@ns="fedramp"]
(11-1)External Point of Contact ...:
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//person-name
  AND Phone Number:
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//phone
(11-1) Connection Security:
  /*/system-implementation/interconnection[1]/annotation[@name="connection-
  security"][@ns="fedramp"]/@value
(11-1) Connection Security - Remark (required if "other"):
  /*/system-implementation/interconnection[1]/annotation[@name="connection-
  security"][@ns="fedramp"]/remarks
(11-1)Data Direction:
  /*/system-implementation/interconnection[1]/prop[@name="direction"][@ns="fedramp"]
(11-1) Information Being Transmitted:
  /*/system-implementation/interconnection[1]/prop[@name="information"][@ns="fedramp"]
(11-1)Port or Circuit Numbers:
  /*/system-implementation/interconnection[1]/prop[@name="port"][@ns="fedramp"]
  OR:
  /*/system-implementation/interconnection[1]/prop[@name="circuit"][@ns="fedramp"]
(13-3) Authorized Connections Information System Name:
  /*/system-implementation/interconnection[1]/remote-system-name
(13-3)Name of Organization CSP Name System Connects To [same as (11-1) External Org Name]:
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//org-name
(13-3) Role of Person Who Signed Connection Agreement
  /*/metadata/role[@id=/*/system-implementation/interconnection[1]/responsible-party/@role-
  id]/title
(13-3) Name of Person Who Signed Connection Agreement [same as (11-1)]
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//person-name
(11-1) POC Phone Number:
  /*/metadata/party[@id=/*/system-implementation/interconnection[1]/responsible-party/party-
  id]//phone
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

12. LAWS, REGULATIONS, STANDARDS AND GUIDANCE

12.1. Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: Templates.

Table 12-1. Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12-1. Information System Name Laws and Regulations

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

12.2. Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: Templates

Table 12-2. Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12-2. Information System Name Standards and Guidance

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

4.30. Laws, Regulations, Standards and Guidance

Representation

```
<back-matter>
   <citation id="cit-1">
      <target>https://domain.example/path/to/document.pdf</target>
      <title>[SAMPLE]Name or Title of Document</title>
      <prop name="type" ns="fedramp">law</prop>
      <prop name="ref-id" ns="fedramp">Identification Number</prop>
      <prop name="publication" ns="fedramp">Document Date</prop>
   </citation>
   <citation id="cit-2">
      <target>https://domain.example/path/to/document.pdf</target>
      <title>[SAMPLE]Name or Title of Document</title>
      <prop name="type" ns="fedramp">guidance</prop>
      <prop name="ref-id" ns="fedramp">Identification Number</prop>
      <prop name="publication" ns="fedramp">Document Date</prop>
   </citation>
   <!-- repeat citation assembly for each law, regulation, standard or guidance -->
   <!-- resource -->
</back-matter>
```

FedRAMP Extensions & Accepted Values

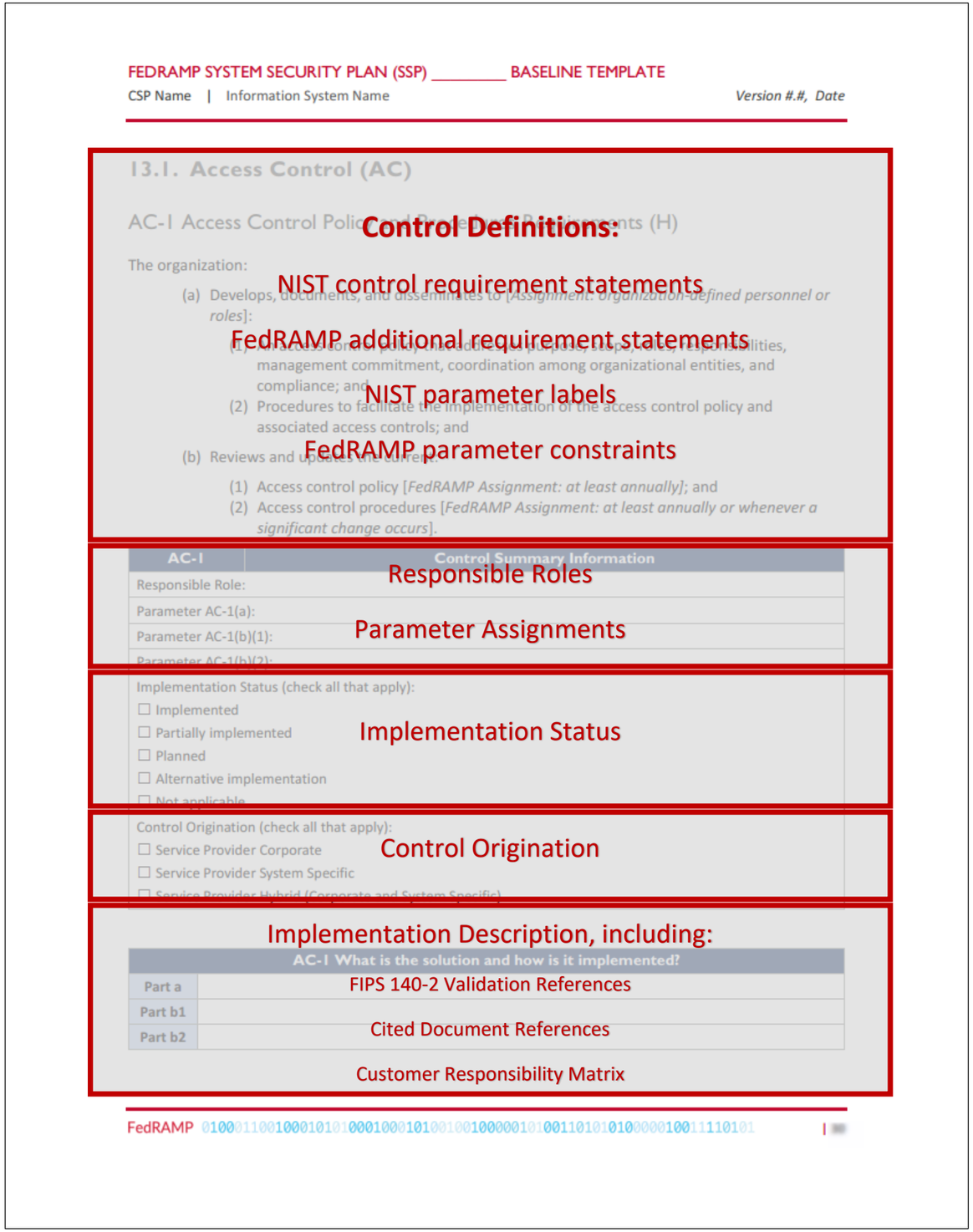
prop (`ns="fedramp"`):

- `name="type"`
  - **Valid:** `law, regulation, standard, guidance`
- `name="ref-id"`
- `name="publication"`

XPath Queries

Replace "[1]" with "[2]", "[3]", etc.

```
Number of Laws and Regulations:
  count(/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])

Laws and Regulations - Identification Number:
  (/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])[1]/../prop[@name="ref-id"][@ns="fedramp"]

Laws and Regulations - Title:
  (/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])[1]/../title

Laws and Regulations - Date:
  (/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])[1]/../prop[@name="publication"][@ns="fedramp"]

Laws and Regulations - Link:
  (/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])[1]/../target

For Standards and Guidance replace "law" with "standard" and "regulation" with
  "guidance" in the above queries.
```



5. SECURITY CONTROLS

This section describes the modeling security control information in an OSCAL-based FedRAMP SSP. To ensure consistent processing, FedRAMP imposes specific requirements on the use of OSCAL for control implementation information.

The modeling of controls is addressed on the following pages in four separate sections as follows:

- **Control Definitions**
- **Responsible Roles and Parameter Assignments**
- **Implementation Status**
- **Control Origination**
- **Implementation Descriptions**

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-8 System Use Notification (L) (M) (H)

The information system:

(a) Displays to users [*Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

(1) Users are accessing a U.S. Government information system;
(2) Information system usage may be monitored, recorded, and subject to audit;
(3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
(4) Use of the information system indicates consent to monitoring and recording;

(b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

(c) For publicly accessible systems:

(1) Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;
(2) Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
(3) Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

FedRAMP 0100011001000101010001000101001001000001010011010101000001001111010 | 48

5.1. Control Definitions

All control definition information is imported from the appropriate FedRAMP profile (baseline). This includes the original NIST control definition and parameter labels, as well as any FedRAMP requirement additions, and parameter constraints.

Interpreting and presenting profile content is beyond the scope of this document. Please refer to the NIST OSCAL Profile and Catalog schema references for more information:

- Profile Model
- Catalog Reference

Only the control implementation information is present within an OSCAL-based SSP. Each control in the FedRAMP baseline must have a corresponding implemented-requirement assembly in the control-implementation assembly.

Representation

```
<!-- metadata -->
<import-profile href="https://path/to/xml/FedRAMP_MODERATE-baseline_profile.xml"/>
<!-- system-characteristics -->
<!-- system-implementation -->
<control-implementation>
   <description><p></p></description>
   <implemented-requirement control-id="ac-1" />
   <implemented-requirement control-id="ac-2" />
   <implemented-requirement control-id="ac-2.1" />
   <!-- cut -->
</control-implementation>
<!-- back-matter -->
```

XPath Queries

Replace "ac-1" with target control ID.

```
URI to Profile:
  /*/import-profile/@href

CSP's Control Implementation Information
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]
```

NOTE:

- FedRAMP tools check to ensure there is one `implemented-requirement` assembly for each control identified in the FedRAMP baseline.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	

Implementation Status (check all that apply):

- ☐ Implemented
- ☐ Partially implemented
- ☐ Planned
- ☐ Alternative implementation
- ☐ Not applicable

Control Origination (check all that apply):

- ☐ Service Provider Corporate
- ☐ Service Provider System Specific
- ☐ Service Provider Hybrid (Corporate and System Specific)
- ☐ Configured by Customer (Customer System Specific)
- ☐ Provided by Customer (Customer System Specific)
- ☐ Shared (Service Provider and Customer Responsibility)
- ☐ Inherited from pre-existing FedRAMP Au… enter text., Date of Authorization

See Next Pages

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.2. Responsible Roles and Parameter Assignments

Every control must have at least one `responsible-role` defined. There must be a separate `responsible-role` assembly for each responsible role. OSCAL requires the specified `role-id` to be valid in the defined list of `roles` in the `metadata`.

FedRAMP further requires the specified role-id must also have been referenced in the `system-implementation`/`user` assembly. This equates to the FedRAMP requirement of all responsible roles appearing in the Personnel Roles and Privileges table.

There must be one `set-parameter` statement for each of the control's parameters, as specified in the FedRAMP baseline. The only exception to this is with nested parameters. Some Select parameters contain an assignment parameter within them, such as appears in AC-7 (b). In these instances, only the final selected value must be provided. The nested assignment parameter may be ignored.

Representation

```
<metadata>
   <role id="role-admin-unix">
      <title>Unix Administrator</title>
      <desc>This is a sample role.</desc>
   </role>
</metadata>

<!-- Fragment: -->
<system-implementation>
   <user id="sys-role-1">
      <role-id>role-admin-unix</role-id>
   </user>
</system-implementation >

<!-- system-implementation -->
<control-implementation>
   <implemented-requirement control-id="ac-1">
      <!-- cut -->
      <responsible-role role-id="role-admin-unix" />
      <set-param param-id="ac-1_prm_a">
         <value>System Manager, System Architect, ISSO</value>
      </set-param>
      <!-- cut -->
</control-implementation>
<!-- back-matter -->
```

XPath Queries

Replace "ac-1" with target control ID.

```
Number of specified Responsible Roles:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/responsible-role)

Responsible Role:
  /*/metadata/role[@id=/*/control-implementation/implemented-requirement[@control-
  id="ac-1"]/responsible-role[1]/@role-id]/title

Check for existence in Personnel Roles and Privileges (Should return a number > 0)
  count(/*/system-implementation/user/role-id[text()=/*/control-
  implementation/implemented-requirement[@control-id="ac-1"]/responsible-role/@role-id])

Parameter Value:
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]/set-
  param[@param-id="ac-1_prm_1"]/value
```

Replace "[1]" with "[2]", "[3]", etc.

Replace "ac-1_prm_1" with target parameter ID.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply):	
☐ Implemented	
☐ Partially implemented	
☐ Planned	
☐ Alternative implementation	
☐ Not applicable	
Control Origination (check all that apply):	
☐ Service Provider Corporate	
☐ Service Provider System Specific	
☐ Service Provider Hybrid (Corporate and System Specific)	
☐ Configured by Customer (Customer System Specific)	
☐ Provided by Customer (Customer System Specific)	
☐ Shared (Service Provider and Customer Responsibility)	
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

See Previous Page

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

See Next Pages

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

5.3. Implementation Status

FedRAMP only accepts only one of five values for `implementation-status`: `implemented`, `partial`, `planned`, `alternative`, and `na`. A control may be marked "partial" and "planned" (using two separate `implementation-status` fields). All other choices are mutually exclusive.

If the status is `partial`, there must also be an annotation (`name="partial" ns="fedramp"`) field containing a description of the gap.

If the status is `planned`, there must also be a prop (`name="planned-completion-date" ns="fedramp"`) field containing the intended completion date, and an annotation (`name="planned" ns="fedramp"`) field containing a brief description of the plan to address the gap, including major milestones.

If the status is `na`, there must also be an annotation (`name="na" ns="fedramp"`) field justifying the N/A status.

Implementation Status Representation

```
<!-- system-implementation -->
<control-implementation>
   <implemented-requirement control-id="ac-1">
      <prop name="implementation-status">implemented</prop>
      <prop name="implementation-status">partial</prop>
      <prop name="implementation-status">planned</prop>
      <prop name="implementation-status">alternative</prop>
      <prop name="implementation-status">na</prop>
      <prop name="planned-completion-date" ns="fedramp">Completion Date</prop>
      <annotation name="partial" ns="fedramp">
         <remarks><p>Describe the unsatisfied gap.</p></remarks>
      </annotation>
      <annotation name="planned" ns="fedramp">
         <remarks><p>Describe the plan to complete the implementation.</p></remarks>
      </annotation>
      <annotation name="na" ns="fedramp">
         <remarks><p>Justification for marking control Not Applicable.</p></remarks>
      </annotation>
      <!-- responsible-role -->
   </control-implementation>
   <!-- back-matter -->
```

FedRAMP Extensions

prop (`ns="fedramp"`):

- `name="planned-completion-date"`

annotation (`ns="fedramp"`):

- `name="partial"`
- `name="planned"`

FedRAMP Accepted Values

`prop name="implementation-status"`:

- implemented, partial, planned, alternate, na

Implementation Status XPath Queries

```
Implementation Status (may return more than 1 result for a given control):
  /*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/prop[@name="implementation-status"][not(@ns)]

Gap Description (If implementation-status="partial"):
  /*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/annotation[@name="partial"][@ns="fedramp"]/remarks

Planned Completion Date (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]/prop[@name="planned-
  completion-date"][@ns="fedramp"]

Plan for Completion (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/annotation[@name="planned"][@ns="fedramp"]/remarks

Not Applicable (N/A) Justification (If implementation-status="na"):
  /*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/annotation[@name="na"][@ns="fedramp"]/remarks
```

Replace "ac-1" with target control-id.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

See Previous Pages

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

See Next Pages

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

5.4. Control Origination

FedRAMP accepts only one of five values for `control-origination`: `sp-corporate`, `sp-system`, `customer-configured`, `customer-provided`, and `inherited`. Hybrid choices are now expressed by identifying more than one `control-origination`, each in a separate prop field. For controls with a control-id ending in "-1", only `sp-corporate`, and `sp-system` are valid.

If the control origination is `inherited`, there must also be a prop (`name="leveraged-authorization" ns="fedramp"`) field containing the Leveraged Authorization ID of the appropriate system as it appears in the `/*/system-characteristics/leveraged-authorization` assembly.

Control Origination Representation

```
<system-characteristics>
   <!-- status -->
   <leveraged-authorization id="lva-1" name="NCName">
      <!-- details cut -- see Leveraged Authorizations Section -->
   </leveraged-authorization>
</system-characteristics>
<!-- system-implementation -->



<control-implementation>
   <implemented-requirement control-id="ac-1">
      <prop name="control-origination">sp-system</prop>
      <prop name="control-origination">inherited</prop>
      <prop name="leveraged-authorization-id" ns="fedramp">lva-1</prop>
      <annotation name="customer-responsibility" ns="fedramp">
         <remarks><p>Describe the customer's responsibilities.</p></remarks>
      </annotation>
   <!-- responsible-role -->
</control-implementation>
<!-- back-matter -->
```

FedRAMP Extensions

prop (`ns="fedramp"`):

- `name="leveraged-authorization-id "`

annotation (`ns="fedramp"`):

- `name="customer-responsibility"`

FedRAMP Accepted Values

`prop name="control-origination"`:

- `sp-corporate, sp-system, customer-configured, customer-provided, inherited`

XPath Queries

```
Number of Control Originations:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/prop[@name="control-origination"][not(@ns)])

Control Origination(could return more than 1 result):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]/prop[@name="control-
  origination"][not(@ns)][1]

Inherited From: System Name (If control-origination="inherited"):
  /*/system-characteristics/leveraged-authorization[@id=/*/control-implementation/implemented-
  requirement[@control-id="ac-1"]/prop[@name="leveraged-authorization-
  id"][@ns="fedramp"]]/annotation[@name="system-name"][@ns="fedramp"]/@value

Inherited From: Authorization Date (If control-origination="inherited"):
  /*/system-characteristics/leveraged-authorization[@id=/*/control-implementation/implemented-
  requirement[@control-id="ac-1"]/prop[@name="leveraged-authorization-
  id"][@ns="fedramp"]]/date-authorized

Customer Responsibility Description
  (If control-origination="customer-configured" or "customer-provided"):
  /*/control-implementation/implemented-requirement[@control-id="ac-
  1"]/annotation[@name="customer-responsibility"][@ns="fedramp"]/remarks
```

Replace "[1]" with "[2]", "[3]", etc.

Replace "ac-1" with target control-id.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.5. Control Implementation Description

The OSCAL file must contain one `implemented-requirement` assembly for each part specified in the existing FedRAMP SSP Templates. For most controls and enhancements in the FedRAMP Baselines based on NIST SP 800-53, Revision 4, this translates as follows:

- **Policy and Procedure Statements**: For each of the -1 controls, such as AC-1, there must be exactly three:
  - `ac-1_smt.a`
  - `ac-1_smt.b.1`
  - `ac-1_smt.b.2`
- **Multi-Part Statement**: If there are outlined parts in the control requirement (a., 1., b., 2., etc.), such as with AC-2, the `control-id` points to the first-level, lettered statements (control-id="ac-2_smt.a"), and there must be one for each lettered statement.
- **Single Statement**: If there is no outlined parts in the control requirement (no a, b, etc.), such as with AC-3, the `control-id` points to the top-level statement (control-id="ac-3_smt"), and there must be exactly one.

Policy and Procedure Representation

```
<!-- system-implementation -->
<control-implementation>
   <!-- cut -->
   <implemented-requirement control-id="ac-1">
      <statement statement-id="ac-3_stmt">
      </statement>
</control-implementation>
<!-- back-matter -->
```

Multi-Part Statement Representation

```
<!-- system-implementation -->
<control-implementation>
   <!-- cut -->
   <implemented-requirement control-id="ac-2">
      <statement statement-id="ac-2_stmt.a" />
      <statement statement-id="ac-2_stmt.b" />
      <!-- cut c, d, e, f, g, h, i -->
      <statement statement-id="ac-2_stmt.j" />
      <statement statement-id="ac-2_stmt.k" />
</control-implementation>
<!-- back-matter -->
```

Single-Statement Representation

```
<!-- system-implementation -->
<control-implementation>
   <!-- cut -->
   <implemented-requirement control-id="ac-3">
      <statement statement-id="ac-3_stmt">
      </statement>
</control-implementation>
<!-- back-matter -->
```

FedRAMP may change this when NIST SP 800-53 Revision 5 is published in 2020.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

5.5.1. Component Approach

NIST has introduced a component-based approach to control satisfaction in OSCAL; however, they are still refining it. FedRAMP is initially making limited use of this approach in order to reduce the transition burden from existing MS Word-based SSPs to OSCAL-based SSPs. **See *Appendix D: Working with Components* for more information.**

Within each of the `statement` assembly FedRAMP prefers all responses appear in one of three `by-component` assemblies as follows:

- **Service Provider Origin** (`component-id="comp-system"`): Describe **how** the service provider is satisfying the control requirement.
- **Inherited** (`component-id="comp-fedramp-authorized-provider-1"`): Describe what is being inherited from the provider. If there is more than one leveraged authorization (not typical), be sure to define a component for each underlying system and use the correct component-id here. If this specific statement is inheriting from more than one provider, list each as a separate `by-component` assembly.
- **Customer Responsibility** (`component-id="comp-customer"`): Describe any customer responsibilities here.

Representation

```
<!-- system-implementation -->
<control-implementation>
   <!-- cut -->
   <implemented-requirement control-id="ac-2">
      <statement statement-id="ac-2_stmt.a">
         <description><p>Ignore.</p></description>
         <!-- Service Provider Responsibility -->
         <by-component component-id="comp-system">
            <description>
               <p>How is the service provider satisfying the control</p>
            </description>
         </by-component>
         <!-- Inherited -->
         <by-component component-id="comp-fedramp-authorized-provider-1">
            <description><p>What is inherited?</p></description>
         </by-component>
         <!-- Customer Responsibility -->
         <by-component component-id="comp-customer">
            <description>
               <p>What must the customer configure or provide?</p>
               <p>This will appear in the Customer Responsibility Matrix.</p>
            </description>
         </by-component>
      </statement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

SEE NEXT PAGE

Tool vendors should expect to see this component approach expand in the future and may want to design tools with this in mind. Contact the NIST OSCAL Team (oscal@nist.gov) or the FedRAMP PMO (info@fedramp.gov) for more information.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.5.2. XPath Queries for Control Implementation Descriptions

XPath Queries

```
Description of How the Service Provider is Satisfying the Requirement :
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id="comp-
  system"]/description
```

Replace "ac-2" with target control-id.

```
Description of WHAT is Inherited:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id="comp-fedramp-
  authorized-provider-1"]/description
```

Replace "ac-2_stmt.a" with target control statement-id.

```
Description of Customer Responsibilities:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_stmt.a"]/by-component[@component-id="comp-
  customer"]/description
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. ***Example*** Enter Information System Abbreviation ***A1 ISPP xx v1.0***. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	. enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA (if needed)	Enter Information System Abbreviation A4 PIA v1.0	. enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	. enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	. enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	. enter extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	. enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	. enter extension

FedRAMP 0100011100100010101000100010100100100000101001101010100001001111010 |

6. ATTACHMENTS

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

ATTACHMENT	MACHINE READABLE	HOW TO HANDLE
Policies and Procedures	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-policy-1"` for policies, and set type to "`policy`". Use `resource id="att-procedure-1"` for procedures, and set type to "`procedure`".
User Guide	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-guide-1"` for guides, and set type to "`guide`".
Digital Identity Worksheet	Yes	Incorporated above. See the *Digital Identity Determination* Section.
Privacy Threshold Analysis (PTA)	Yes	Incorporated into System Information. See the *Privacy Impact Assessment* Section.
Privacy Impact Assessment (PIA)	No (Future)	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-pia"`. FedRAMP intends to incorporate machine-readable PIA content into the OSCAL-based FedRAMP SSP at a later date.
Rules of Behavior	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-rob"` for procedures, and set type to "`rob`".
Information System Contingency Plan	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-plan-cp"` for procedures, and set type to "`plan`".
Configuration Management Plan	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-plan-cm"` for procedures, and set type to "`plan`".
Incident Response Plan	No	Attach using the `back-matter`, `resource` syntax. Use `resource id="att-plan-ir"` for procedures, and set type to "`plan`".
CIS Workbook	Yes	This can be generated from the content in the Security Controls section and no longer needs to be maintained separately or attached.
FIPS-199	Yes	Incorporated above. See the *Security Objectives Categorization (FIPS-199)* Section.
Inventory	Yes	See the *System Inventory* Section below.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. ***Example*** Enter Information System Abbreviation ***A1 ISPP xx v1.0***. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	. enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA (if needed)	Enter Information System Abbreviation A4 PIA v1.0	. enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	. enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	. enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	. enter extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	. enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	. enter extension

6.1. Attachments

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

Attachment Representation

```
<!-- cut -->
<back-matter>
   <!-- citation -->
   <resource id="att-policy-1">
      <desc>Policy document</desc>
      <prop name="type" ns="fedramp">policy</prop>
      <prop name="title" ns="fedramp">Document Title</prop>
      <prop name="publication" ns="fedramp">Document Date</prop>
      <prop name="version" ns="fedramp">Document Version</prop>
      <!-- Add rlink with relative path or embed with base64 encoding -->
      <base64>00000000</base64>
   </resource>
   <resource id="att-policy-2" />
   <!-- cut: policies 3 - 13 -->
   <resource id="att-policy-14" />
   <resource id="att-procedure-1" />
   <!-- cut: procedure 2 - 13 -->
   <resource id="att-policy-14" />
   <resource id="att-guide-user" />
   <resource id="att-rob" />
   <resource id="att-plan-cp" />
   <resource id="att-plan-cm" />
   <resource id="att-plan-ir" />
</back-matter>
```

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp"`):

- `name="type"`
  - **Valid:** policy, procedure, guide, pia, rob, plan
- `name="title"`
- `name="publication"`
- `name="version"`

XPath Queries

```
The Number of Policies Attached:
  count(/*/back-matter/resource/prop[@name="type"][@ns="fedramp"][text()="policy"])

Attachment (Embedded Base64 encoded):
  /*/back-matter/resource[@id="att-policy-1"]/base64
  OR (Relative Link):
  /*/back-matter/resource[@id=""]/rlink/@href

Title of First Policy Document:
  /*/back-
  matter/resource/prop[@name="type"][@ns="fedramp"][text()="policy"]/../prop[@name="title"][@
  ns="fedramp"]
```

Replace "policy" with "plan", "rob", etc. for each attachment type.

ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

Privacy Overview and Point of Contact (POC)

The Table 15-6. Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

Table 15-6. Information System Name; Privacy POC

Name	Click here to enter text.
Title	Click here to enter text.
CSP / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

6.2. Privacy Impact Assessment: POC

Much of the Privacy Impact Assessment (PIA) is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations.

Attachment Representation

```
<!-- cut -->
<metadata>
   <role id="role-system-privacy-officer">
      <title>Privacy Official's Point of Contact</title>
      <desc>The individual responsible for the PTA and if necessary the PIA.</desc>
   </role>
   <!-- cut -->
   <party id="person-007">
      <person>
         <person-name>[SAMPLE]Person Name 7</person-name>
         <org-name>CSP Name</org-name>
         <address>
            <addr-line>Suite 0000</addr-line>
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
         </address>
         <email>name@org.domain</email>
         <phone>000-000-0000</phone>
         <prop name="title" ns="fedramp">Individual's Title</prop>
      </person>
   </party>
   <!-- cut -->
   <responsible-party role-id="role-system-privacy-officer">
      <party-id>person-007</party-id>
   </responsible-party>
   </role>
</metadata>
```

XPath Queries

```
POC Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-privacy-
  officer"]/party-id]]/*/person-name

POC Org Name:
  /*/metadata/party[@id=[/*/metadata/responsible-party[@role-id="role-system-privacy-
  officer"]/party-id]]/*/org-name

NOTE: Replace "org-name" with "phone", "email", "addr-line", "city", "state", or "zip" as
  needed. There may be more than one "addr-line"
```

ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

Table 15-7. <Information System Name> Laws and Regulations

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

6.3. Privacy Impact Assessment: Laws and Regulations

Much of the Privacy Impact Assessment (PIA) is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations.

Attachment Representation

```
<!-- cut -->
<back-matter>
   <citation id="cit-2">
      <target>https://domain.example/path/to/document.pdf</target>
      <title>[SAMPLE]Privacy-Related Law Citation</title>
      <prop name="type" ns="fedramp">law</prop>
      <prop name="type" ns="fedramp">pii</prop>
      <prop name="ref-id" ns="fedramp">Identification Number</prop>
      <prop name="publication" ns="fedramp">Publication Date</prop>
   </citation>
</back-matter>
```

XPath Queries

```
Number of Privacy Laws and Regulations:
  count((/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])/../prop[@name="type"][@ns="fedramp"][(text() = "pii")])

Privacy Laws and Regulations - Identification Number:
  ((/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])/../prop[@name="type"][@ns="fedramp"][(text() =
  "pii")])[1]/../prop[@name="ref-id"][@ns="fedramp"]

Laws and Regulations - Title:
  ((/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])/../prop[@name="type"][@ns="fedramp"][(text() = "pii")])[1]/../title

Privacy Laws and Regulations - Date:
  ((/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])/../prop[@name="type"][@ns="fedramp"][(text() =
  "pii")])[1]/../prop[@name="publication"][@ns="fedramp"]

Privacy Laws and Regulations - Link:
  ((/*/back-matter/citation/prop[@name="type"][@ns="fedramp"][(text() = "law") or
  (text()="regulation")])/../prop[@name="type"][@ns="fedramp"][(text() =
  "pii")])[1]/../target
```

Replace "[1]" with "[2]", "[3]", etc.

ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

QUALIFYING QUESTIONS

Select One	1.	Does the ISA collect, maintain, or share PII in any identifiable form?
Select One	2.	Does the ISA collect, maintain, or share PII information from or about the public?
Select One	3.	Has a Privacy Impact Assessment ever been performed for the ISA?
Select One	4.	Is there a Privacy Act System of Records Notice (SORN) for this ISA system? If yes; the SORN identifier and name is: Enter SORN ID/Name.

If answers to Questions 1-4 are all "No" then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment.

DESIGNATION

Check one.

☐ A Privacy Sensitive System

☐ Not a Privacy Sensitive System (in its current version)

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: Templates.

6.4. Privacy Impact Assessment: Designation and Qualifying Questions

Attachment Representation

```
<!-- cut -->
<system-characteristics>
   <system-information>
      <!-- Attachment 4, PTA/PIA Designation -->
      <prop name="privacy-sensitive" class="pta" ns="fedramp">yes</prop>
      <!--Does the ISA collect, maintain, or share PII in any identifiable form? -->
      <prop name="pta-1" class="pta" ns="fedramp">yes</prop>
      <!--Does the ISA collect, maintain, share PII info from or about the public? -->
      <prop name="pta-2" class="pta" ns="fedramp">yes</prop>
      <!--Has a Privacy Impact Assessment ever been performed for the ISA? -->
      <prop name="pta-3" class="pta" ns="fedramp">yes</prop>
      <!--Is there a Privacy Act System of Records Notice (SORN) for this ISA system? -->
      <prop name="pta-4" class="pta" ns="fedramp">yes</prop>
      <prop name="pta-sorn-id" class="pta" ns="fedramp">[No SORN ID]</prop>
      <!-- information-type -->
   </system-information>
</system-characteristics>
```

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp", class="pta"`):

- `name="privacy-sensitive"`
  - **Valid:** yes, no
- `name="pta-1"`
  - **Valid:** yes, no
- `name="pta-1"`
  - **Valid:** yes, no
- `name="pta-1"`
  - **Valid:** yes, no
- `name="sorn-id"`

XPath Queries

```
Privacy Designation (yes = Privacy Sensitive):
  /*/system-characteristics/system-information/prop[@name="privacy-sensitive"][@ns="fedramp"]

Qualifying Question #1:
  /*/system-characteristics/system-information/prop[@name="pta-1"][@ns="fedramp"]

Qualifying Question #2:
  /*/system-characteristics/system-information/prop[@name="pta-2"][@ns="fedramp"]

Qualifying Question #3:
  /*/system-characteristics/system-information/prop[@name="pta-3"][@ns="fedramp"]

Qualifying Question #4:
  /*/system-characteristics/system-information/prop[@name="pta-4"][@ns="fedramp"]

Qualifying Question #4:
  /*/system-characteristics/system-information/prop[@name="sorn-id"][@ns="fedramp"]
```

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

OS/Infrastructure Inventory								
NetBIOS Name	**MAC Address**	**Authenticated Scan**	**Baseline Configuration Name**	**OS Name and Version**	**Location**	**Asset Type**	**Hardware Make/Model**	**In Latest Scan**
If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Is the asset is planned for an authenticated scan?	If available, provide the name of the configuration template used within the CSP configuration management.	Operating System Name and Version running on the asset.	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)	Name of the hardware product and model.	Should the asset appear in the network scans and can it be probed by the scans creating the current POA&M?
Valid NetBIOS name.	Valid MAC Address.	Yes or No.	.		Valid locations for CSP infrastructure.	Do not use vendor or product names which should go in Columns N (for hardware) or Columns P-Q for software or database.		Yes or No.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Optional for OS/Infrastructure. Leave blank for Software and Database.	Optional for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.

Software and Database Inventories				
Software/ Database Vendor	**Software/ Database Name & Version**	**Patch Level**	**Function**	**Comments**
Name of Software or Database vendor.	Name of Software or Database product and version number.	If applicable.	For Software or Database, the function provided by the Software or Database for the system.	Any additional information that could be useful to the reviewer.
If open source (e.g., there is no "vendor), enter "Open Source" as the vendor name.				
Mandatory for Software and Database. Leave blank for OS/Infrastructure.	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	Optional if applicable. Otherwise, leave blank.	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	Optional for OS/Infrastructure, Software and Database.

6.5. System Inventory: Components

Attachment Representation

```
<!-- cut -->
<system-implementation>
   <!-- user -->
   <component id="comp-fips-1" name="[SAMPLE]Module Name" component-type="validation">
      <description><p>[SAMPLE]FIPS 140-2 Validated Module</p></description>
      <prop name="cert-no" ns="fedramp">0000</prop>
      <link href="https://csrc.nist.gov/ ...cut... /Certificate/0000" />
      <status state="operational" />
   </component>

   <component id="comp-validated-product-1"
      name="[SAMPLE]Product Name" component-type="software" >
      <description><p>FUNCTION: Describe typical component function.</p></description>
      <prop name="asset-type" ns="fedramp">os</prop>
      <prop name="scan-type" ns="fedramp">os</prop>
      <prop name="vendor-name" ns="fedramp">Vendor Name</prop>
      <prop name="model" ns="fedramp">Model #</prop>
      <prop name="version" ns="fedramp">Version Number</prop>
      <prop name="patch-level" ns="fedramp">Patch Level</prop>
      <prop name="validation-link" ns="fedramp">comp-fips-module-1</prop>
      <status state="operational" />
      <remarks><p>COMMENTS: Provide other comments as needed.</p></remarks>
   </component>
   <!-- Repeat the component assembly for each component -->
   <!-- service -->
   <!-- interconnection -->
   <!-- system-inventory -->
</system-implementation>
```

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp"`):

- `name="asset-type"`
  - **Valid:** See Registry
- `name="scan-type"`
  - **Valid:** os, inf, db, web
- `name="vendor-name "`
- `name="model"`
- `name="version"`
- `name="patch-level"`
- `name="validation-link"`

XPath Queries

SEE NEXT PAGE

NOTES:

- Patch Level, Function, and Comments may appear in the component or inventory-item assembly. Every inventory-item must either directly provide a function description or be linked to a component that provides a function description.
- The `component-type` for all physical infrastructure devices should be set to "hardware", with the `asset-type` containing "router", "switch", etc.
- The `component type` for all non-physical inventory items should be set to "software", with the `asset-type` containing, "os", "database", "webserver", "dns", etc.
- Initially FedRAMP will be more flexible about the above designations until these concepts have been applied by CSPs and real-world exceptions analyzed.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

OS/Infrastructure Inventory								
NetBIOS Name	**MAC Address**	**Authenticated Scan**	**Baseline Configuration Name**	**OS Name and Version**	**Location**	**Asset Type**	**Hardware Make/Model**	**In Latest Scan**
If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Is the asset is planned for an authenticated scan?	If available, provide the name of the configuration template used within the CSP configuration management.	Operating System Name and Version running on the asset.	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)	Name of the hardware product and model.	Should the asset appear in the network scans and can it be probed by the scans creating the current POA&M?
Valid NetBIOS name.	Valid MAC Address.	Yes or No.	.		Valid locations for CSP infrastructure.	Do not use vendor or product names which should go in Columns N (for hardware) or Columns P-Q for software or database.		Yes or No.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Optional for OS/Infrastructure. Leave blank for Software and Database.	Optional for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.

Software and Database Inventories				
Software/ Database Vendor	**Software/ Database Name & Version**	**Patch Level**	**Function**	**Comments**
Name of Software or Database vendor.	Name of Software or Database product and version number.	If applicable.	For Software or Database, the function provided by the Software or Database for the system.	Any additional information that could be useful to the reviewer.
If open source (e.g., there is no "vendor), enter "Open Source" as the vendor name.				
Mandatory for Software and Database. Leave blank for OS/Infrastructure.	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	Optional if applicable. Otherwise, leave blank.	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	Optional for OS/Infrastructure, Software and Database.

XPath Queries

```
Number of Hardware Components:
  count(/*/system-implementation/component[@component-type="hardware"])

Number of Software Components:
  count(/*/system-implementation/component[@component-type="software"])

Vendor Name:
  /*/system-implementation/component[@component-type="software"][1]/prop[@name="vendor-
  name"][@ns="fedramp"]

Product Name:
  /*/system-implementation/component[@component-type="hardware"][1]/@name

Model:
  /*/system-implementation/component[@component-
  type="hardware"][1]/prop[@name="model"][@ns="fedramp"]

Version:
  /*/system-implementation/component[@component-
  type="software"][1]/prop[@name="version"][@ns="fedramp"]

Patch Level:
  /*/system-implementation/component[@component-type="software"][1]/prop[@name="patch-
  level"][@ns="fedramp"]

Asset Type:
  /*/system-implementation/component[@component-type="software"][1]/prop[@name="asset-
  type"][@ns="fedramp"]

Scan Type:
  /*/system-implementation/component[@component-type="software"][1]/prop[@name="scan-
  type"][@ns="fedramp"]

FIPS 140-2 Validation Certificate Number:
  /*/system-implementation/component[@id=/*/system-implementation/component[@component-
  type="software"][1]/prop[@name="validation-link"][@ns="fedramp"]]/prop[@name="cert-
  no"][@ns="fedramp"]

FIPS 140-2 Link to Validation Information:
  /*/system-implementation/component[@id=/*/system-implementation/component[@component-
  type="software"][1]/prop[@name="validation-link"][@ns="fedramp"]]/link/@href
```

Replace "[1]" with "[2]", "[3]", etc.

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

All Inventories			
IPv4 or IPv6 Address	**Virtual**	**Public**	**DNS Name or URL**
If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.	Is this asset virtual?	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.
	Yes or No.	Yes or No.	Valid DNS name or URL.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure, Software, and Database.	Mandatory for OS/Infrastructure, Software, and Database.	Optional, unless used as Identifier in vulnerability scans or security assessments.

Any Inventory				
Comments	**Serial #/Asset Tag#**	**VLAN/ Network ID**	**System Administrator/ Owner**	**Application Administrator/ Owner**
Any additional information that could be useful to the reviewer.	Product serial number or internal asset tag #.	Virtual LAN or Network ID.	Name of the system administrator or owner.	Name of the application administrator or owner.
Optional for OS/Infrastructure, Software and Database.	Optional for OS/Infrastructure, Software, and Database.	Optional for OS/Infrastructure, Software, and Database.	Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	Optional for OS/Infrastructure, Software, and Database.

6.5.1. Inventory Items

Attachment Representation

```
<!-- cut -->
<system-implementation>
   <!-- interconnection -->
   <system-inventory>
      <inventory-item id="inv-1" asset-id="asset-tag-or-serial-#">
         <description><p>If needed, describe this instance.</p></description>
         <prop name="address-ipv4" ns="fedramp">0.0.0.0</prop>
         <prop name="address-ipv6" ns="fedramp">0000:0000:0000:0000</prop>
         <prop name="address-mac" ns="fedramp">00:00:00:00:00:00</prop>
         <prop name="virtual" ns="fedramp">no</prop>
         <prop name="public" ns="fedramp">no</prop>
         <prop name="dns" ns="fedramp">dns.name</prop>
         <prop name="url" ns="fedramp">uniform.resource.locator</prop>
         <prop name="netbios" ns="fedramp">netbios-name</prop>
         <prop name="baseline-name" ns="fedramp">Baseline Configuration Name</prop>
         <prop name="location" ns="fedramp">Physical location of Asset</prop>
         <prop name="patch-level" ns="fedramp">Patch-Level</prop>
         <annotation name="scan-authenticated" ns="fedramp" value="no">
            <remarks><p>If no, explain why. If yes, omit remark.</p></remarks>
         </annotation>
         <annotation name="scan-latest" ns="fedramp" value="yes">
            <remarks><p>If no, explain why. If yes, omit remark.</p></remarks>
         </annotation>
         <responsible-party role-id="asset-owner">
            <party-id>party-it-dept</party-id>
         </responsible-party>
         <responsible-party role-id="asset-admin">
            <party-id>party-it-dept</party-id>
         </responsible-party>
         <implemented-component component-id="comp-router-1" />
         <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
      </inventory-item>
   <!-- Repeat the inventory-item assembly for each item in the inventory -->
   </system-inventory>
   <!-- system-implementation remarks -->
</system-implementation>
```

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

XPath Queries

SEE NEXT PAGE

FedRAMP Extensions & Accepted Values

prop (`ns="fedramp"`):

- `name="address-ipv4"`
- `name="address-ipv6"`
- `name="address-mac"`
- `name="virtual"`
  - **Valid:** yes, no
- `name="public"`
  - **Valid:** yes, no
- `name="dns"`
- `name="url"`
- `name="netbios"`
- `name="baseline-name"`
- `name="patch-level"`

annotation (`ns="fedramp"`):

- `name="scan-authenticated"`
  - **Valid:** yes, no
- `name="scan-latest"`
  - **Valid:** yes, no

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

All Inventories			
IPv4 or IPv6 Address	**Virtual**	**Public**	**DNS Name or URL**
If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.	Is this asset virtual?	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.
	Yes or No.	Yes or No.	Valid DNS name or URL.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure, Software, and Database.	Mandatory for OS/Infrastructure, Software, and Database.	Optional, unless used as Identifier in vulnerability scans or security assessments.

Any Inventory				
Comments	**Serial #/Asset Tag#**	**VLAN/ Network ID**	**System Administrator/ Owner**	**Application Administrator/ Owner**
Any additional information that could be useful to the reviewer.	Product serial number or internal asset tag #.	Virtual LAN or Network ID.	Name of the system administrator or owner.	Name of the application administrator or owner.
Optional for OS/Infrastructure, Software and Database.	Optional for OS/Infrastructure, Software, and Database.	Optional for OS/Infrastructure, Software, and Database.	Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	Optional for OS/Infrastructure, Software, and Database.

XPath Queries

```
Number of Inventory Items:
  count(/*/system-implementation/system-inventory/inventory-item)

Asset ID (Asset Tag# or Serial #):
  /*/system-implementation/system-inventory/inventory-item[1]/@asset-id

IPv4 Address (may be more than one):
  /*/system-implementation/system-inventory/inventory-item[1]/prop[@name="address-
  ipv4"][@ns="fedramp"]

MAC Address (may be more than one):
  /*/system-implementation/system-inventory/inventory-item[1]/prop[@name="address-
  mac"][@ns="fedramp"]

Virtual:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="virtual"][@ns="fedramp"]

Public:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="public"][@ns="fedramp"]

DNS Name:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="dns"][@ns="fedramp"]

URL:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="url"][@ns="fedramp"]

NetBIOS Name:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="netbios"][@ns="fedramp"]

Location:
  /*/system-implementation/system-inventory/inventory-
  item[1]/prop[@name="location"][@ns="fedramp"]

Patch Level:
  /*/system-implementation/system-inventory/inventory-item[1]/prop[@name="patch-
  level"][@ns="fedramp"]

Comments:
  /*/system-implementation/system-inventory/inventory-item[1]/remarks

Authenticated Scan:
  /*/system-implementation/system-inventory/inventory-item[1]/annotation[@name="scan-
  authenticated"][@ns="fedramp"]/@value

Authenticated Scan Justification (if Authenticate Scan is "no"):
  /*/system-implementation/system-inventory/inventory-item[1]/annotation[@name="scan-
  authenticated"][@ns="fedramp"]/remarks

Latest Scan:
  /*/system-implementation/system-inventory/inventory-item[1]/annotation[@name="scan-
  latest"][@ns="fedramp"]/@value

Latest Scan Justification (if Authenticate Scan is "no"):
  /*/system-implementation/system-inventory/inventory-item[1]/annotation[@name="scan-
  latest"][@ns="fedramp"]/remarks
```

Replace "[1]" with "[2]", "[3]", etc.

APPENDIX A. OSCAL-BASED FEDRAMP BASELINES

The system's identified security categorization level governs which FedRAMP baseline applies. This can be checked using the XPath syntax below.

Security Sensitivity Level XPath Query

```
Security Categorization Level:
  /*/system-characteristics/security-sensitivity-level
```

This determines which URL should be entered for the `import-profile` field in an OSCAL-based FedRAMP SSP.

Baseline Representation

```
    <!-- metadata -->
    <!-- This must point to the appropriate FedRAMP Baseline -->
    <import-profile href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml"/>
    <!-- system-characteristics -->
```

FedRAMP validation tools will compare the identified security categorization level to the actual FedRAMP baseline specified in the SSP and raise a warning if a different baseline was used.

High

XML Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_HIGH-baseline_profile.xml

JSON Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_HIGH-baseline_profile.json

Moderate

XML Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_MODERATE-baseline_profile.xml

JSON Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_MODERATE-baseline_profile.json

Low

XML Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_LOW-baseline_profile.xml

JSON Version:
https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_LOW-baseline_profile.json

Do not copy and modify the FedRAMP baseline. FedRAMP will use the original, published file for validation, ignoring any modified copies.

If you require a modification to the FedRAMP baselines, such as may be required when directed to do so by an authorizing official, first contact FedRAMP to coordinate the modification, then follow the instructions in Appendix B.

FedRAMP Tailored

FedRAMP Tailored for Low Impact – Software as a Service (LI-SaaS) Appendix B merges SSP, SAP, and SAR information into a single document. The SSP portions of that document may be represented using the same OSCAL conventions described in this document with only a few minor differences.

Fully representing Appendix B in OSCAL requires syntax that has not yet been developed. For these reasons, a separate guide will be developed for FedRAMP Tailored once the appropriate syntax has been defined.

For your convenience, FedRAMP has made the FedRAMP Tailored for LI-SaaS baseline available now in both XML and JSON formats as follows:

Low-Impact SaaS (Tailored)
XML Version: https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/xml/FedRAMP_LI-SaaS-baseline_profile.xml **JSON Version:** https://raw.githubusercontent.com/usnistgov/OSCAL/master/content/fedramp.gov/json/FedRAMP_LI-SaaS-baseline_profile.json

APPENDIX B. MODIFYING A FEDRAMP BASELINE

OSCAL is designed to allow modification of controls and baselines, while maintaining traceability through each layer of modification. This means you should never copy and modify a FedRAMP baseline.

If you require a change to a FedRAMP baseline, you should first coordinate that change with the FedRAMP JAB or PMO. Assuming FedRAMP agrees with the change, the correct way to implement the change is as follows:

1. **Create a new, blank OSCAL Profile.**
2. **Point to the FedRAMP Baseline**: Point it to the appropriate FedRAMP baseline using an `import` field.
3. **Select the Relevant Controls**: Use the `include` and `exclude` fields to identify the controls to include or exclude from the FedRAMP baseline.
   a. For example, if you need all but one control, you can `include all`, then `exclude` the one.
4. **Specify How Controls Are Organized**: FedRAMP prefers you merge "as-is" using those merge fields. This is relevant when resolving the profile. See the *Profile Resolution* section of this appendix for more information.
5. **Modify the Selected Controls**: Use the `modify` assembly to make modifications to parameters and control definitions.

The next page contains an example profile, which accomplishes the following actions:

- Imports the FedRAMP Moderate baseline
- Includes all controls from that baseline
- Explicitly removes AT-4 from the baseline
- Indicates that if this profile is resolved the organization of the controls should remain as-is. See the *Profile Resolution* section of this appendix for more information.
- Adds a constraint to the third parameter of AC-1 (ac-1_prm_3), which is more restrictive than the FedRAMP constraint, but changing it from "at least annually" to "at least every six months".
- Removes the additional FedRAMP requirement statement in AU-11 and replaces it with a more restrictive statement, which now requires online retention of audit records for at least 180 days instead of 90 days.

For more information on working with profiles, please visit the NIST OSCAL site at:
https://pages.nist.gov/OSCAL

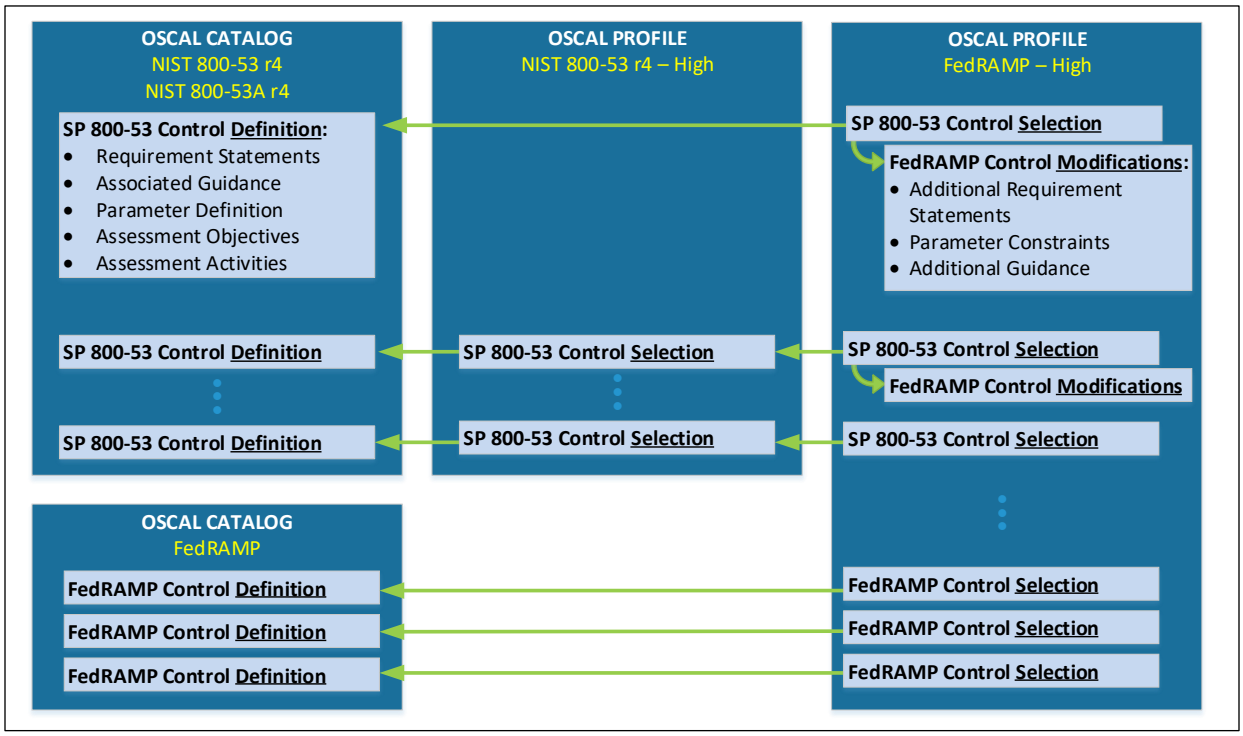
A complete OSCAL profile syntax reference is available here:
https://pages.nist.gov/OSCAL/documentation/schema/profile/

Sample Profile to Modify a FedRAMP Baseline

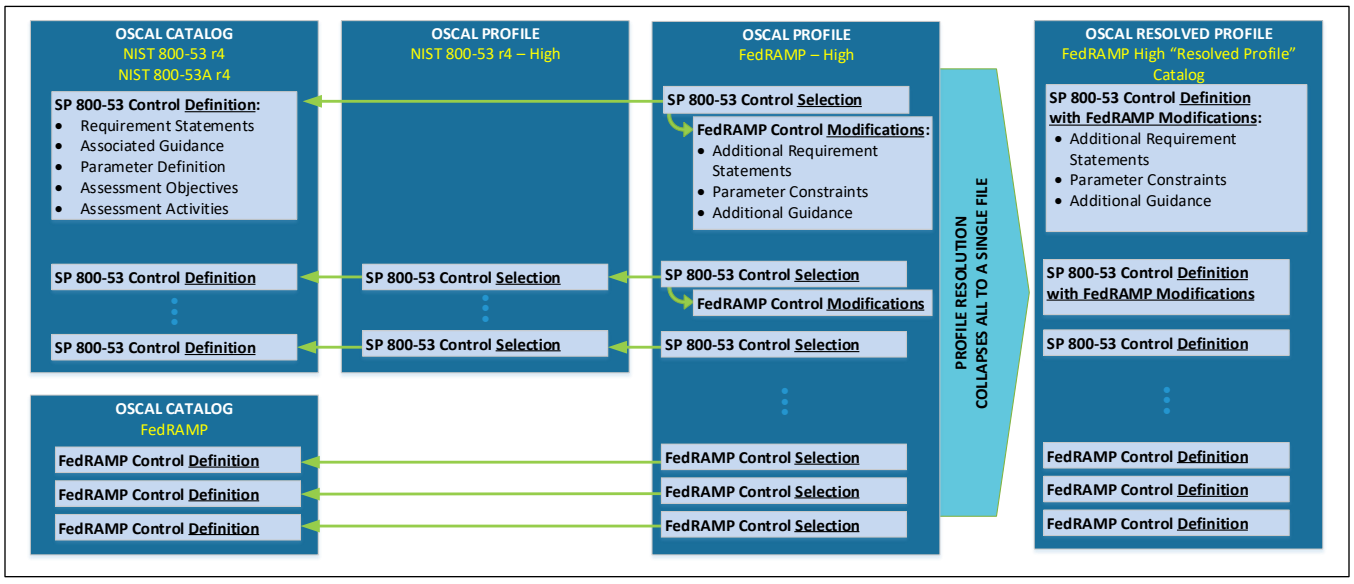
```
<profile xmlns="http://csrc.nist.gov/ns/oscal/1.0"
      id="uuid-xxxx">
      <metadata>
            <title>[XYZ Org] Modification to FedRAMP Moderate
Baseline</title>
            <last-modified>2019-10-01T11:03:27.392-04:00</last-modified>
            <version>1.1</version>
            <oscal-version>1.0.0-milestone2</oscal-version>
      </metadata>
      <import href="https://path/to/FedRAMP_MODERATE-baseline_profile.xml">
            <include>
                  <!-- Include every control in the Moderate baseline -->
                  <all with-child-controls="yes" />
            </include>
            <exclude>
                  <!-- Remove Control AT-4 -->
                  <call control-id="at-4" />
            </exclude>
      </import>
      <merge><as-is>yes</as-is></merge>
      <modify>
            <set param-id="ac-1_prm_3">
                  <!-- Change the constraint from "at least annually" -->
                  <constraint>at least every six months</constraint>
            </set>
            <remove id-ref="au-11_fr" />
            <alter control-id="au-11">
                  <add position="ending">
                        <part id="au-11_fr" name="item" ns="fedramp">
                              <title>[XYZ Org]Modified Requirement</title>
                              <part id="au-11_fr_smt.1" name="item">
                                    <prop name="label">Requirement:</prop>
                                    <p>The service provider retains audit
records on-line for at 180 days and further preserves audit records off-line
for a period that is in accordance with NARA requirements.</p>
                              </part>
                        </part>
                  </add>
            </alter>
      </modify>
</profile>
```

Profile Resolution

Profiles are intended to identify upstream sources of control definition information and show only the changes to those upstream sources. This enables humans and computers to trace control definition changes back to their source framework.



An organization may prefer to work with a single, complete file containing only the final set of relevant control definitions. OSCAL provides a process for merging this collection of catalogs and profiles into a single catalog. This process is called "profile resolution".



The `merge` assembly within an OSCAL profile offers a profile creator control over how the final file is organized. To maintain the same organization, simply use the `as-is` field and set it to "yes".

The complete profile syntax is available here:
https://pages.nist.gov/OSCAL/documentation/schema/profile/

APPENDIX C. WORKING WITH ROLES, PEOPLE, AND ORGANIZATIONS

An OSCAL SSP file defines roles, people, and organizations within the metadata as part of three separate assemblies:

- **`role`**: A role ID and role title are required. Other content, such as a short-name, description, or remarks are optional.
- **`party`**: People and organizations are defined next as parties. An organization is any collection of people, and can represent a company, agency, department, or team.
- **`responsible-party`**: Links roles to parties. The same role can have more than one party assigned to it. Also a party can be assigned to more than one role.

Working with Role Identifiers

All roles within the document are defined under the metadata element as follows:

```
<metadata>
   --- cut ---
   <role id="role-ssp-by">
      <title>Prepared By</title>
      <desc>The organization that prepared this SSP.</desc>
   </role>
   <role id="role-ssp-for">
      <title>Prepared For</title>
      <desc>The organization for which this SSP was prepared</desc>
   </role>
   --- cut ---
</metadata>
```

To ensure consistent processing, FedRAMP has defined a specific set of roles that must exist with a FedRAMP SSP with the provided role identifiers. **Most are pre-populated in the OSCAL-based FedRAMP SSP Template.** CSPs must ensure these roles, titles, and descriptions exist within an OSCAL-based FedRAMP SSP. CSPs may add additional roles, provided these roles remain.

FedRAMP-defined role-identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.

FedRAMP Defined Party Identifiers

To ensure consistent processing, FedRAMP has defined a specific set of party identifiers that must exist with a FedRAMP SSP with the provided party identifiers. **Some are pre-populated in the OSCAL-based FedRAMP SSP Template.** CSPs must ensure these party identifiers are used where appropriate. CSPs may assign their own details to these parties; however, FedRAMP's systems will search for the defined party using these IDs.

FedRAMP-defined party identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.

APPENDIX D. WORKING WITH COMPONENTS

NIST designed OSCAL such that a system architect expresses all aspects of the system as components. There are several ways to use components in an OSCAL-based SSP. The following defines FedRAMP's initial use.

This section will likely be updated as NIST continues to evolve its approach to components in OSCAL.

FedRAMP-defined component identifiers are cited in relevant portions of this document, and summarized in the FedRAMP OSCAL Registry.

Minimum Required Components

There must be a component that represents the entire system itself, and has the ID "`comp-system`", as well as a component that represents customers.

The following is an example of defined components. The first three are required; the forth is an example.

Minimum Required Component Representation

```
<!-- system-characteristics -->
<system-implementation>
   <!-- user -->

   <!-- This System -->
   <component id="comp-system" name="This System" component-type="system" >
      <description><p>
         The entire system as depicted in the system authorization boundary.
      </p></description>
      <status state="operational" />
   </component>

   <!-- Customer -->
   <component id="comp-customer" name="Customer" component-type="customer" >
      <description><p>Customer's Responsibility</p></description>
      <status state="other" />
   </component>
</system-implementation>
```

Common Additional Components

If there is an underlying FedRAMP-authorized system, from which the subject system is inheriting controls, there must be a component for that as well, with the ID "`comp-fedramp-authorized-provider-1`".

For each FIPS 140-2 validated module, there must be a component that represents the validation certificate itself. For more information about this, see the *FIPS 140-2 Validated Components* Section.

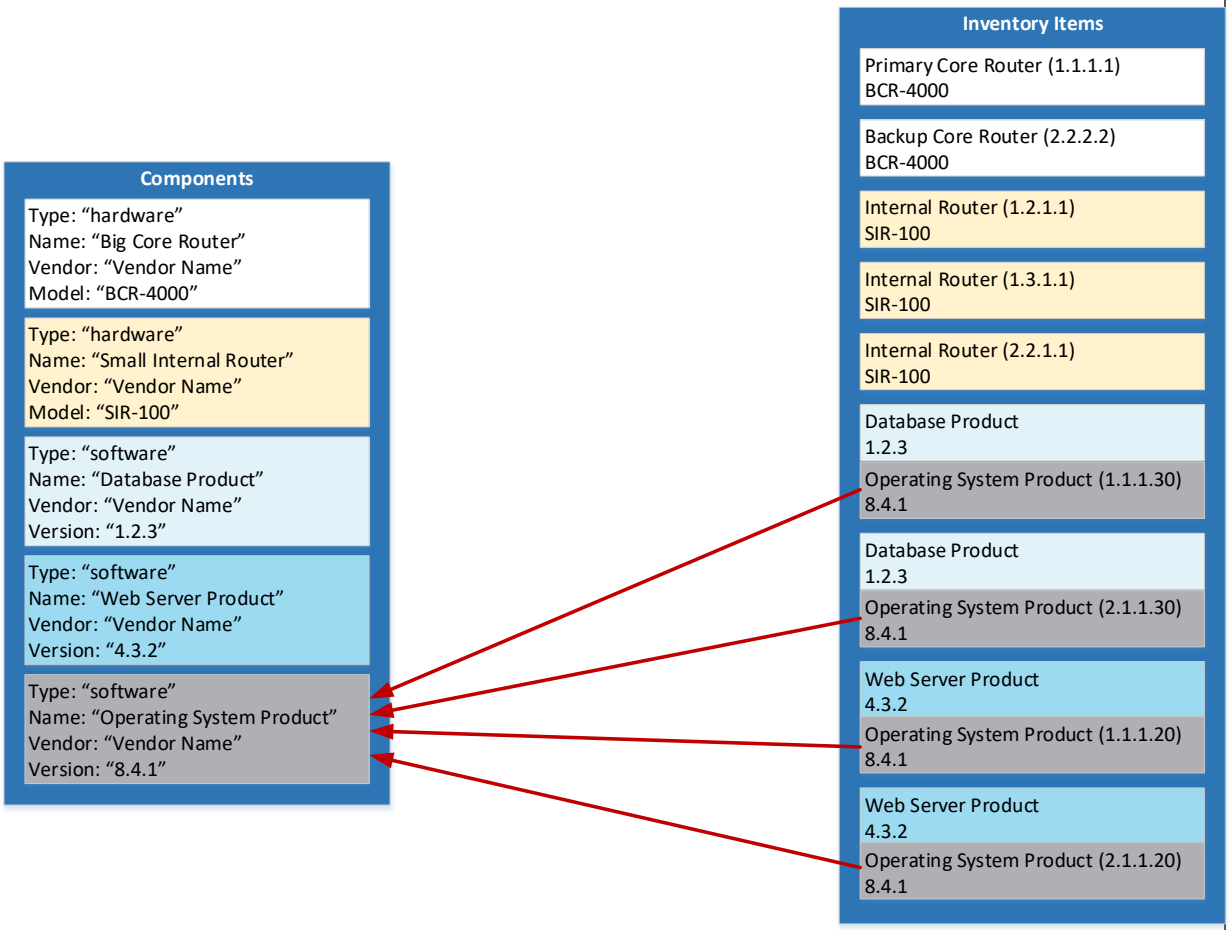
Common Additional Component Representation

```
   <!-- system-characteristics -->
   <system-implementation>
      <!-- user -->
      <!-- Minimum Required Components -->

      <!-- Leveraged FedRAMP-authorization system -->
      <component id="comp-fedramp-authorized-provider"
                    name="[Provider System's Name]" component-type="service" >
         <description><p>A FedRAMP-authorized system.</p></description>
         <prop name="authorization-date" ns="fedramp">2019-01-01</prop>
         <status state="operational" />
      </component>

      <!-- FIPS 140-2 Validation Certificate Information -->
      <!-- Include a separate component for each relevant certificate -->
      <component id="comp-fips-module-1" name="Name" component-type="validation">
         <description><p>FIPS 140-2 Validated Module</p></description>
         <prop name="cert-no" ns="fedramp">0000</prop>
         <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" />
         <status state="operational" />
      </component>

      <!-- service -->
   </system-implementation>
   <!-- control-implementation -->
```

Components as a Basis for System Inventory

NIST's approach to component-based system modeling is to reduce redundancy of information and increase flexibility. NIST accomplishes this with separate component and inventory item modeling. This is a one-to-many relationship. One component to many inventory item instances.

For example, if an open source operating system (OS) is used in many places throughout the system, it is defined once as a component. All information about the product, vendor, and support are modeled within the component detail. If the OS is used four times within the system, each use is an inventory item, with details about that specific information, such as IP address,



Relationship of Components and Inventory Items

FedRAMP requires a component assembly for each model of infrastructure device used, and each version of software and database used within the system. FedRAMP is not asking for more detail than provided in the legacy inventory workbook. Only that the information is organized differently.

As NIST continues to evolve its component approach, FedRAMP will re-evaluate its approach to system inventory representation.

FIPS 140-2 Validated Components

NIST's component model treats independent validation of products and services as if that validation were a separate component. This means when using components with FIPS 140-2 validated cryptographic modules:

- **The Validation Definition**: A component definition that provides details about the validation.
- **The Product Definition**: A component definition that describes the hardware or software product.

The validation definition is a component definition that provides details about the independent validation. In the case of FIPS 140-2 validation, this must provide the certificate number, and the link to entry in the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program Database.

In the future, NIST will provide syntax that allows the product and the validation to be linked; however, this syntax is not yet available, so FedRAMP is providing alterative syntax to accomplish the linking.

While FedRAMP requires the separate component definition for FIPS 140-2 validation, linking those components using the FedRAMP extension is optional. Once NIST provides final syntax to link a product and its validation, that link will become mandatory.

Component Representation: Example Product With FIPS 140-2 Validation

```
   <!-- system-characteristics -->
   <system-implementation>
      <!-- user -->
      <!-- Minimum Required Components -->

      <!-- FIPS 140-2 Validation Certificate Information -->
      <!-- Include a separate component for each relevant certificate -->
      <component id="comp-fips-module-1" name="Name" component-type="validation">
         <description><p>FIPS 140-2 Validated Module</p></description>
         <prop name="cert-no" ns="fedramp">0000</prop>
         <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" />
         <status state="operational" />
      </component>

      <!-- FIPS 140-2 Validated Product -->
      <component id="comp-validated-product"
                     name="Product Vendor" component-type="software" >
         <description><p>A product with a cryptographic module.</p></description>
         <status state="operational" />
      </component>

      <!-- service -->
   </system-implementation>
   <!-- control-implementation -->
```